



Informe Prueba a Plan de Recuperación de Desastres Formiik

Informe Prueba a Plan de Recuperación de Desastres

Formiik



Informe Prueba a Plan de Recuperación de Desastres Formiik

OBJETIVO	3
CONTEXTO	3
ARQUITECTURA FORMIIK	4
COMUNICACIÓN CON CLIENTES	5
MEJORAS IMPLEMENTADAS	5
SEGUNDO CLOUDSERVICE (EN OTRA REGIÓN)	5
TRAFFIC MANAGER	7
GEOREPLICACIÓN - FAILOVER SQL AZURE	8
GEOREDUNDANCIA – STORAGE ACCOUNT	10
RESUMEN DE ACTIVIDADES DE LA CERTIFICACIÓN DEL DRP	11
ESCENARIO ALTA DISPONIBILIDAD	12
DISPONIBILIDAD ESCENARIOS BAJA CRITICIDAD	12



Informe Prueba a Plan de Recuperación de Desastres Formiik

Objetivo

Implementar cambios a la configuración y administración de la plataforma Formiik que permita recuperar su funcionalidad al 100% en caso de desastre en un plazo menor a 4 horas a partir de la declaratoria de emergencia.

Contexto

Formiik brinda servicio a poco más de 15,000 usuarios de clientes de Latinoamérica, en la mayoría de las implementaciones el uso de Formiik es de misión crítica para ciertos procesos tales como originación de créditos, verificación de domicilios, cobranza (Sector Microfinanzas), entrega de mercancía, entrega y activación de TC (Sector Logístico-Entregas) por mencionar algunos de ellos.

Formiik se hospeda en la plataforma Azure y para operar requiere de los siguientes componentes principales: Base de Datos (SQL Azure), Computo (CloudService), Almacenamiento (StorageAccount/Blobs-Tables-Queues) estos componentes a su vez residen en una Región (DataCenter).

El escenario en el que el DataCenter quedase fuera de línea por completo rebasaba la posibilidad de reestablecer el servicio en un corto tiempo para la versión 1.2 del Plan de Recuperación de Desastres de Formiik, esto fue evidenciado en el evento del 4 de Septiembre, dado que tenía la dependencia de Acceso a recursos de Azure que bajo la circunstancia de fallo general no están disponibles.

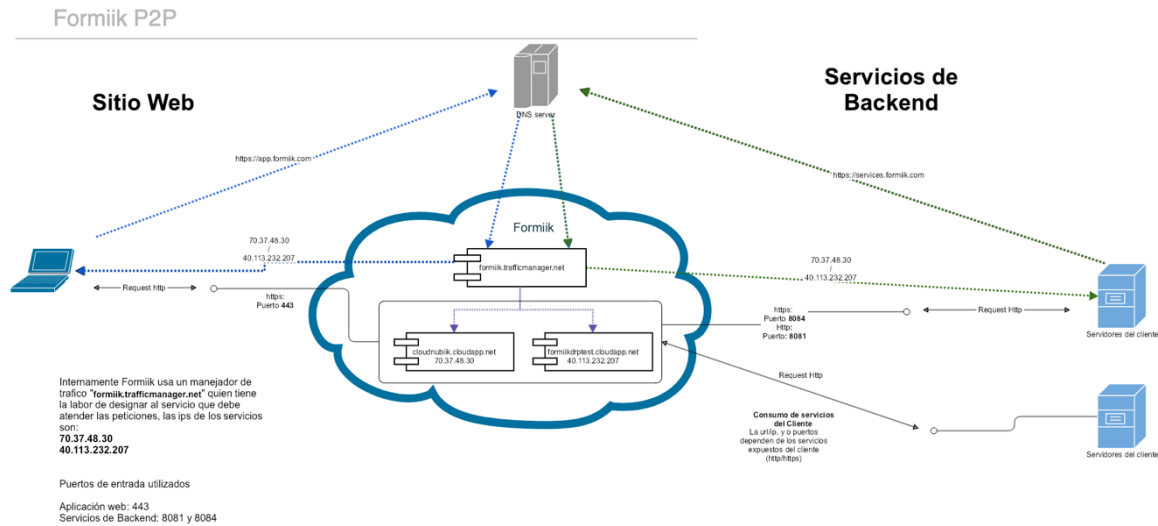
Dicho lo anterior y considerando las opciones que brinda Azure así como la necesidad de nuestros clientes de poder reestablecer operaciones en el menor tiempo posible incluso en caso de falla catastrófica se realizaron las revisiones de documentación y alcances de productos de la plataforma que ayudaran a reducir las horas para recuperar operaciones.

A continuación, se muestra el diagrama de arquitectura del producto en su versión donde reside solo en una región.



Informe Prueba a Plan de Recuperación de Desastres Formiik

Comunicación con Clientes



Mejoras Implementadas

Segundo CloudService (en otra Región)

Al implementar un segundo CloudService (computo distribuido) se tiene la posibilidad de reaccionar ante una eventual contingencia solo modificando el balanceo desde el Traffic Manager y/o desplegando un número mayor de instancias en la Región Alterna para poder procesar las transacciones de los usuarios finales.



Informe Prueba a Plan de Recuperación de Desastres Formiik

PaaS (Platform as a Service)

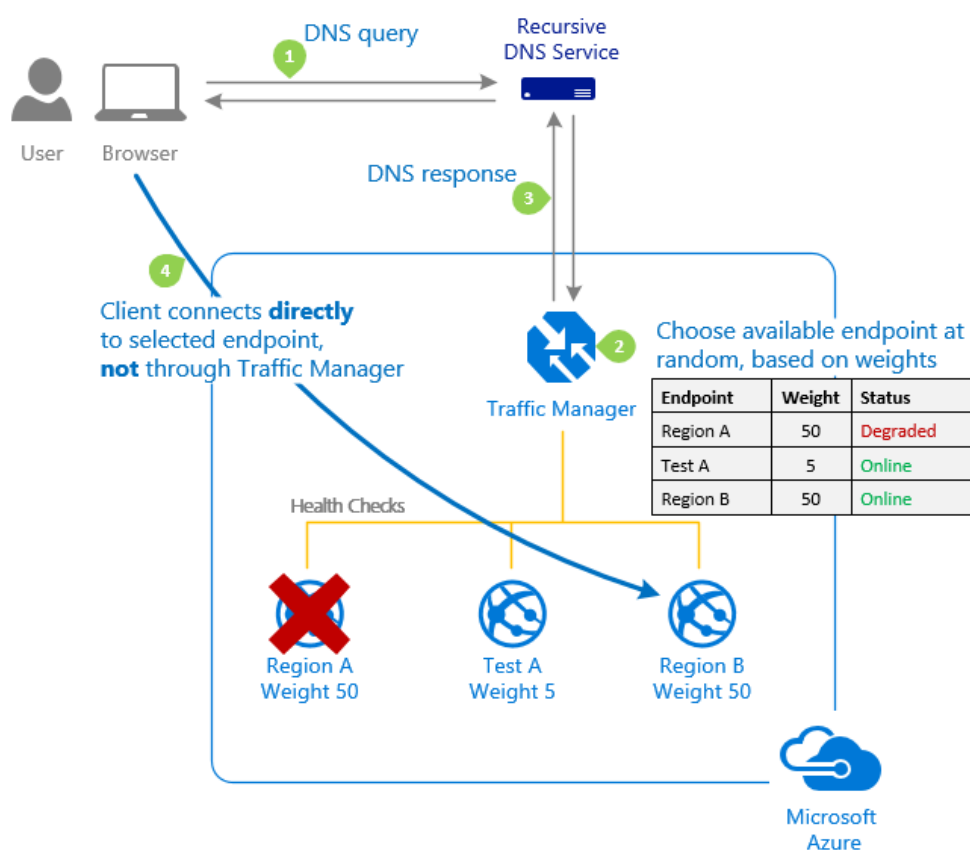




Informe Prueba a Plan de Recuperación de Desastres Formiik

Traffic Manager

Permite a Formiik la posibilidad de balancear el uso del computo distribuido en las 2 regiones.



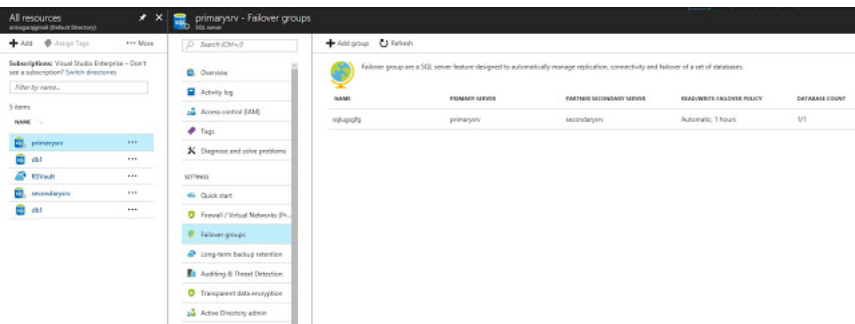
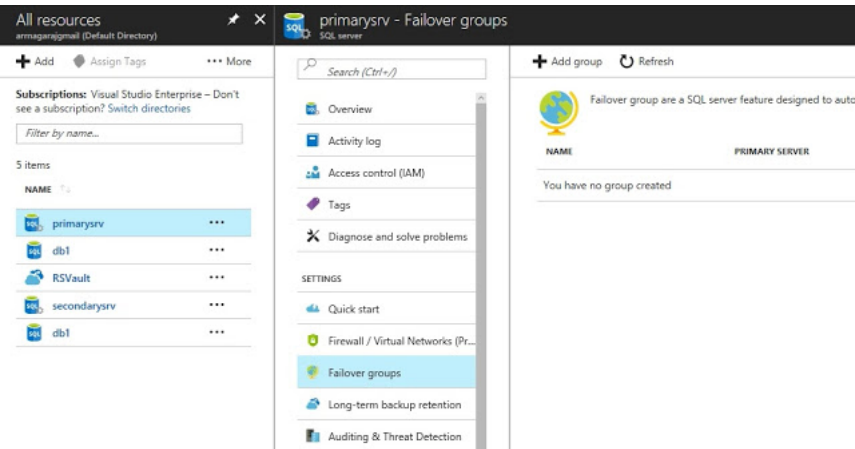


Informe Prueba a Plan de Recuperación de Desastres

Formiik

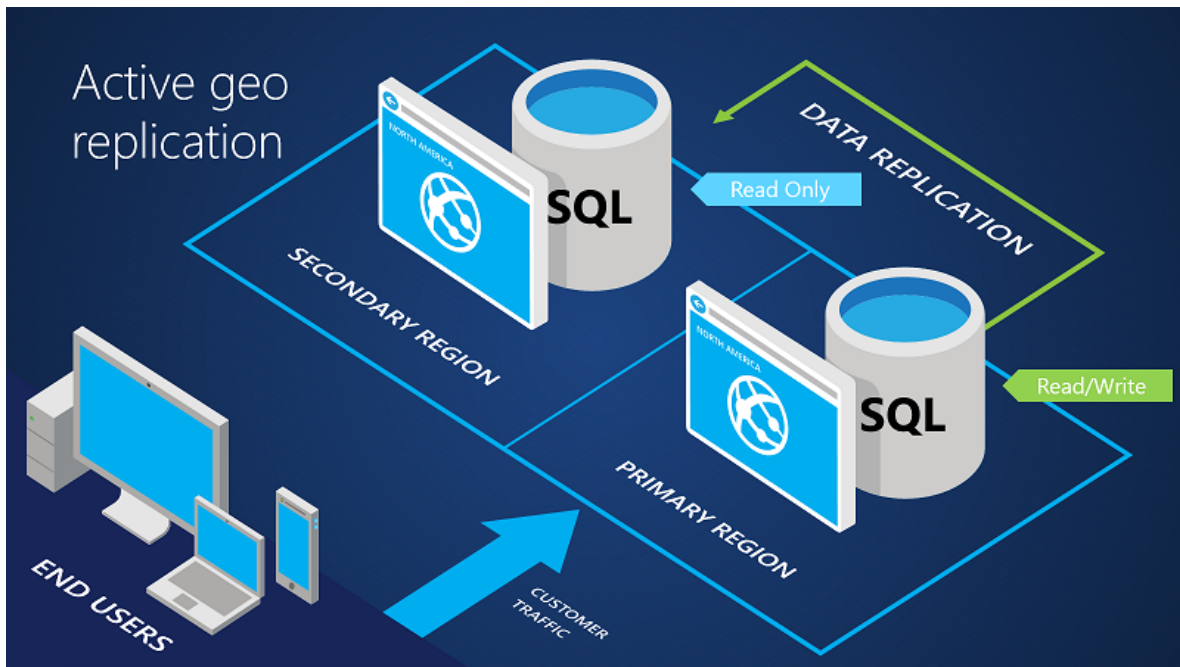
Georeplicación - Failover SQL Azure

Permite la posibilidad de cambiar a un servidor secundario bajo una eventual contingencia y poder volver





Informe Prueba a Plan de Recuperación de Desastres Formiik



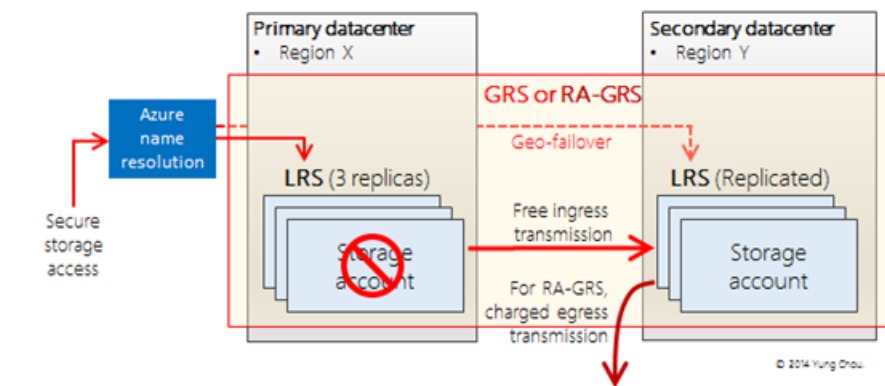


Informe Prueba a Plan de Recuperación de Desastres Formiik

Georedundancia – Storage Account

Permite realizar el cambio hacia otro DataCenter para continuar la operación dado el esquema de replicación

Azure Geo-Redundant Storage (GRS/RA-GRS)





Informe Prueba a Plan de Recuperación de Desastres Formiik

Resumen de Actividades de la Certificación del DRP

- Automatización del despliegue de versión de Formiik para incorporar ambos cloudservice.
- Publicación de un segundo servicio (CloudService) en un Data Center alterno, con los mismos componentes que se describen en el diagrama (web role, workerrole).
- Implementación de la función de Traffic Manager (balanceador)
- Activar georedundancia para los Storageaccount: permitiría mediante un cambio en la configuración de las llaves de acceso poder operar en caso de indisponibilidad de la región principal.
- Configuración de servidores de Base de Datos Secundarios
- Creación de Elastic Pool en los servidores secundarios. (previo a la replicación)
- Configuración de esquema Georeplicación-Failover groups para SQL Azure: permite tener opciones de alta disponibilidad en caso de fallo general en la Región principal.
- Pruebas de ciclo completo en distintos ambientes para asegurar la conectividad desde la aplicación en cada uno de sus funciones.
- Simulación de escenario de Failover para una Base de Datos Productiva
- Pruebas de ciclo completo, con apoyo de usuario final (login, sincronización, consultas flexibles, envió de órdenes, envió de respuestas y visualización en sistemas centrales), consultas desde portal Web y desde Base de datos



Informe Prueba a Plan de Recuperación de Desastres Formiik

- Actualización de Procesos de Contingencia a ejecutar en caso de Desastre, considerando las modificaciones a la arquitectura.
- Actualización de diagrama de arquitectura general del producto

Escenario Alta Disponibilidad

SQL Azure

Tiempo de implementación inicial de Replica: 1hr

Tiempo para hacer Failover: 10-15 minutos (RTO)

RPO <5 s

Almacenamiento

Tiempo para hacer Failover: 20 minutos (RTO)

RPO <10 min

Disponibilidad Escenarios Baja Criticidad

SQL Azure

La base de datos se restaura de un Backup offsite (de un día previo)

RTO < 4 hrs

RPO < 12 hrs

Tiempo para hacer Failover: 20 minutos (RTO)

RPO <10 min