Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Creación de un modelo de recuperación contra desastres costo-efectivo para pymes utilizando computación en la nube.

Presentado por:

Quesada Rivel, Juan

agosto de 2018

Declaración derechos de autor

Agradecimientos

A mi familia:

A mi esposa Laura, mis hijos Santiago y Sebastian por el apoyo incondicional y la motivación de seguir adelante.

Al profesor tutor:

A Cesar Rodriguez por su guía, recomendaciones y notable acompañamiento dentro y fuera de clase.

A la Universidad Cenfotec:

A todo el personal de la Universidad que me recibió con brazos abiertos desde el primer día.

Al Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica (MICITT):

Por el apoyo económico mediante su exitoso programa de becas de innovación y capital humano para la competitividad

Aprobación del tribunal examinador.

“Para uso de la aprobación del proyecto de parte del Tribunal Examinador”

Tabla de Contenido

Capítulo 1 Introducción

Generalidades

El siguiente documento incluye una recopilación de información de dominio público, basada principalmente de sitios web de buena reputación, como universidades y proveedores de tecnología, sobre buenas prácticas en escenarios de recuperación contra desastres utilizando soluciones basadas en computación en la nube para las pequeñas y medianas empresas. A criterio del autor y con base en su experiencia, se seleccionará la información más relevante y se presentará de una manera que le facilite al lector la autoevaluación de conocimiento y la capacidad de implementación de un modelo en la recuperación. La audiencia recomendada son gerencias, arquitectos y demás responsables e interesados en brindar solución a la continuidad del negocio desde la perspectiva tecnológica.

Antecedentes del Problema

Se han analizado las arquitecturas de tecnología de empresas a lo largo de varios años, y se llega a la conclusión de que la mayoría de las empresas carecen de mecanismos seguros para la continuidad de negocio, lo que ha llevado al estudio, diseño y prueba de varias soluciones de recuperación contra desastres que aumentan la calidad de servicio y la seguridad de los sistemas. Debido a la reducida capacidad económica de las pymes, se ha identificado cómo las soluciones de computación en la nube ofrecen un mecanismo de bajo costo estimado en menos de USD$200* al mes que permite a las empresas mantener operación continua. Específicamente el autor se enfocará en soluciones de nube pública de Microsoft llamada Azure, dadas la experiencia y pruebas realizadas con la tecnología que además se integran de manera sencilla con la mayoría de las tecnologías existentes como hipervisores, sistemas operativos y bases de datos sin depender de un software adicional de terceros.

* El dato es calculado basado en las siguientes suposiciones.

- 5 servidores sistema operativo Windows con 2 núcleos y 8GB de memoria RAM promedio por máquina virtual.
- 640GB de almacenamiento promedio.
- Tiempo fuera de línea estimado por mes de 24hrs, para el cálculo del uso de cómputo y conexión VPN.
- 2 direcciones IP Públicas

Microsoft Azure, estimación de costos		
Su presupuesto		
Tipo de servicio	Descripción	Costo estimado mensual
Licencia ASR	5 instancias a Azure, 5 discos S10 (128GB)	$154.44
Computo	5 servidores A4 v2 (4 vCPU; 8 GB de RAM) x 24 horas; Sistema operativo Windows	$34.32
VPN	Puertas de enlace de VPN, nivel VpnGw1, 24 horas de uso, Transferencias de datos 50GB	$6.31
IP Pública	2 direcciones IP Publica estáticas	$5.84
		$200.91
Estimado creado el 6/4/2018 de https://azure.microsoft.com/es-es/pricing/calculator/		

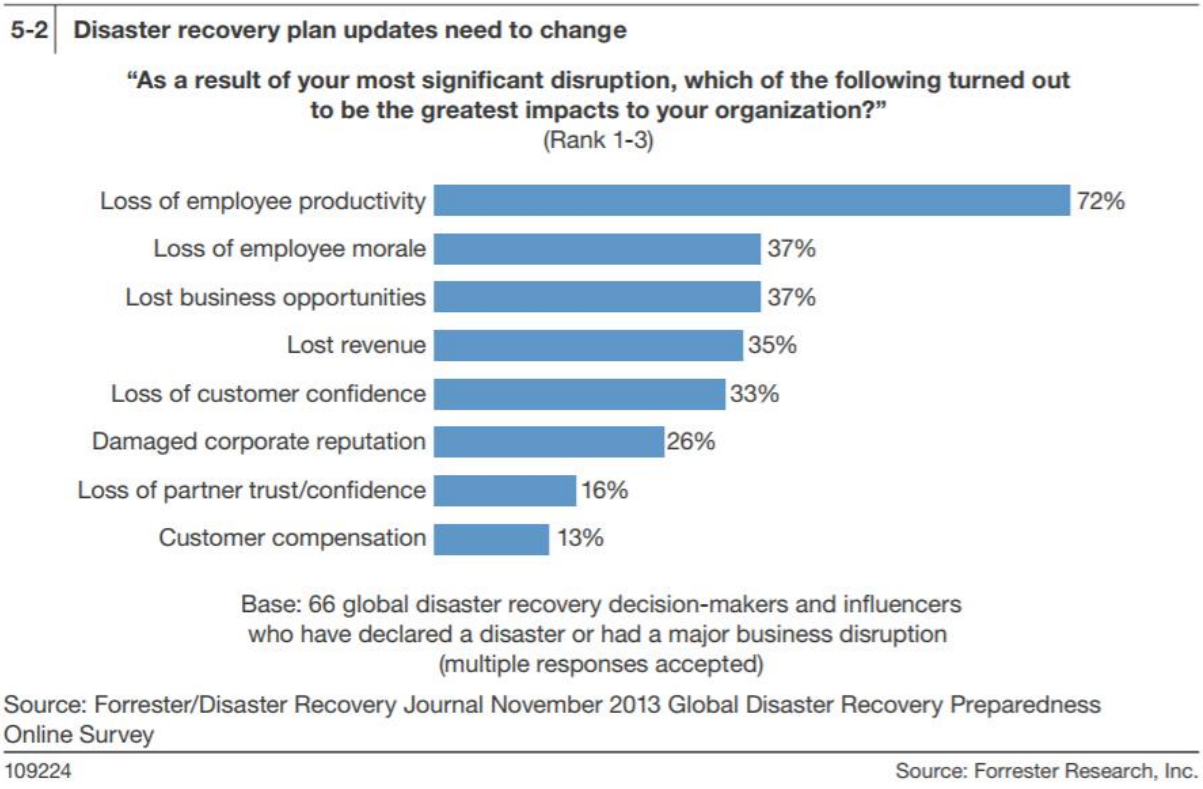
Definición y Descripción del Problema

En un mundo cada vez más digital, la información y los sistemas informáticos se convierten en uno de los activos más valorados por las empresas, la misma representa desde propiedad intelectual, inteligencia de negocio, lista de clientes, hasta la operación. De aquí el valor de que la información sea confidencial, integral y siempre disponible.

La recuperación de desastres es crítica para la continuidad del negocio de las empresas, la alta dependencia de tecnología hace que los sistemas informáticos sean parte integral del negocio en las empresas. La no disponibilidad de los servicios está normalmente ligada a la disminución de productividad, pérdida de capacidad transaccional, disminución de la satisfacción al cliente y afectación de la imagen corporativa que se traduce en pérdidas.

Según estudio de IDC, *"DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified"* para las empresas Fortune 1000 el costo anual promedio por fallos es de 1.5 a 2.5 billones de dólares, es decir el costo por hora de una aplicación crítica fuera de función está entre los $500,000 y $1,000,000. Si bien estos números son de empresas grandes no significa que en proporción las empresas pequeñas no sufren pérdidas; imaginemos un supermercado, librería, farmacia o restaurante, entre otros, con su sistema de cajas sin función por 1 hora, la cantidad de transacciones no procesadas, las colas de clientes enojados con el comercio, los empleados frustrados de no poder realizar su trabajo. Según un estudio de Symantec *"Symantec 2011 SMB Disaster Preparedness Survey*" para Latinoamérica, el costo cuantificado para las pequeñas empresas es de $12,500 por día y para una mediana empresa de $23,000.

Según un estudio por Forrester "The State of Business Continuity Preparedness", el principal impacto se da por la pérdida de productividad y moral de los empleados, pérdidas de dinero y de oportunidades, así como daño a la reputación y pérdida de confianza de los clientes y socios.

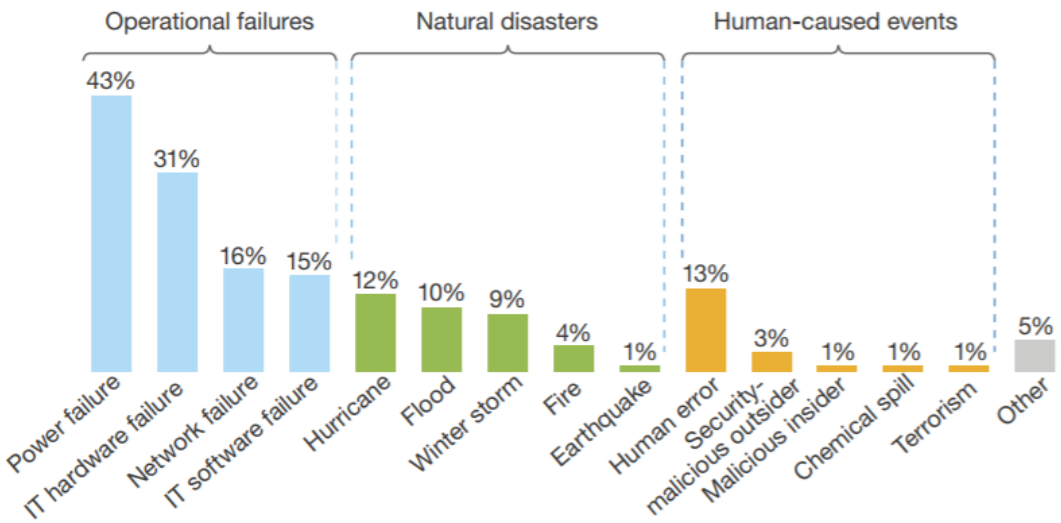


Tradicionalmente las grandes empresas de la industria, como banca y gobierno, son las que han tenido esquemas de recuperación contra desastres avanzados, dado que el costo operativo y capital es muy elevado, esto porque un sitio secundario implica tener un segundo centro de datos, así como todo su equipamiento y operación. Sin embargo, con la introducción de la computación en la nube y soluciones de recuperación de desastres que las mismas ofrecen, las pequeñas y medianas empresas pueden tener un esquema de recuperación de desastres como un gasto operativo a un bajo costo. Pueden así protegerse y operar aun en la falla del centro de datos primario, ya sea por temas operativos como falla de poder y falla de equipos, así como desastres naturales como inundaciones, terremotos o huracanes, sin dejar de lado temas humanos como errores, ataques cibernéticos, negligencia.

En el mismo estudio Forrester calcula los principales incidentes que conllevan a una falla y les da peso a cuáles son los más comunes. Aclaremos que la recuperación contra desastres no se limita a desastres naturales, sino a su amplitud de variables operativas y humanas.

5-1 | Top causes of downtime are mundane events, not disasters

"What was the cause(s) of your most significant disaster declaration(s) or major business disruption?"



Base: 94 global disaster recovery decision-makers and influencers
(does not include "don't know" responses; multiple responses accepted)

En Latinoamérica, con base en la experiencia del autor, el sector de las pymes en su mayoría carece de sistemas de recuperación contra desastres o bien los que tienen son muy básicos. Esto se debe a varias razones como falta de capacidad técnica experimentada, que el departamento de TI se ve como un costo a nivel gerencial y no un beneficio, desconocimiento de posibles soluciones o bien negligencia.

Justificación

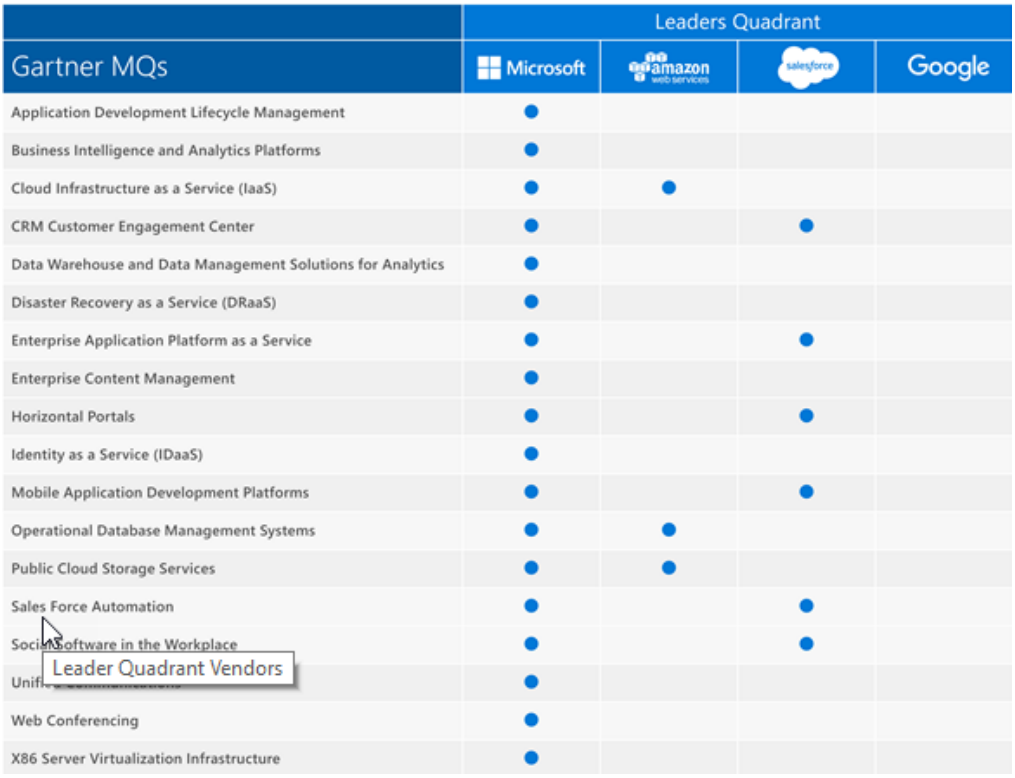
Este documento se enfoca en apoyar aquellas pymes que requieren un esquema de recuperación contra desastres para mantener la continuidad de negocio y así no perder productividad, ventas, dinero, imagen y mantener la calidad del servicio aun en incidentes no esperados. Aunque el gasto económico en tecnologías contra recuperación de desastres es mínimo para ofrecer continuidad de negocio, no se compara con el gasto que puede generar no tener un esquema correcto que en ocasiones puede llevar a pérdidas millonarias. Tomemos como ejemplo la caída del proveedor de Cloud público AWS, el cual, por un error de código, generó pérdidas de más de $150 millones de dólares según la empresa Cyence Inc, en un artículo publicado en el Wall Street Journal. Dicho de otra manera, la no disponibilidad de servicios es un problema de seguridad y la seguridad informática es una prioridad del negocio y no de tecnología, dado su impacto directo al mismo.

Se busca además apoyar a los empresarios a que puedan optar por metodologías y tecnologías innovadoras y costo-efectivas que les permita aumentar su competitividad en el mercado sin sacrificar enfoque a su negocio principal. Normalmente las pymes tienen capacidad técnica limitada, lo que afecta la visión y ejecución en materia de transformación digital, se mantienen pensamientos tradicionales de alta inversión en tecnología y personal para operarlo. Es necesario romper esta barrera para entender que las tecnologías de la información son un aliado en el crecimiento del negocio, porque pueden ayudar a transformar los productos, optimizar las operaciones y transformar la manera cómo comercializar a los clientes.

Para efectos del presente documento, se basará en una solución de computación de nube de Microsoft llamada Azure por múltiples razones, entre ellas Azure posee todas las capacidades tanto en temas de respaldos, así como de recuperación de sitio alterno en sus 50 geografías de manera nativa, además de integración con otros proveedores de software. Microsoft también es el único proveedor de Cloud público que se encuentra en 18 cuadrantes de Gartner como líder superando considerablemente a su segundo competidor,

quien solo participa y no es líder en *Disaster Recovery as a Service o DRaaS, por su traducción al inglés.*

Cuadrantes Gartner comparativos de los líderes en computación en nube



Un factor adicional es que existe un caso de éxito en Costa Rica de esta tecnología, el cual da un excelente punto de referencia. Este es el caso del hospital CIMA, el cual implementó tecnologías de recuperación contra desastres con un resultado muy positivo. “La migración a la nube de Azure también le ha traído a la organización beneficios en la manera en la que se aprovechan y protegen los recursos tecnológicos. Los procesos de backup son sencillos, pues siempre hay espacio disponible y las opciones que ofrece el sistema para su manejo son muy visuales y fáciles de entender” expresó Federico Portugués, jefe del Área de Informática del Hospital CIMA San José

Por último, el autor de este documento es certificado en las tecnologías indicadas, además trabaja para la empresa Microsoft en el área específica, lo cual ofrece mayor nivel de conocimiento y experiencia con las tecnologías a tratar. Esto permite dar mayor profundidad en el tema.

Viabilidad

Como se apreciará a continuación, el proyecto es viable no solamente por la perspectiva técnica, operativa y económica, sino también porque el autor se dedica a desarrollar soluciones que incorporan escenarios de recuperación contra desastres, tanto para pymes como para empresas de larga escala en la región de Latinoamérica. El autor no se encarga como tal de la implementación, pero sí de recopilar necesidades de negocio y capacidades actuales, desarrollar soluciones basadas en los requerimientos del negocio, análisis costo-beneficio de las soluciones, así como interactuar con los proveedores de servicio encargados de llevar a cabo la implementación y operación continua. Además, se cuenta con vasta documentación de herramientas de análisis de costos, arquitecturas de referencia, así como casos de éxitos.

Punto de Vista Técnico

Las tecnologías de computación en la nube, en temas de recuperación contra desastres como respaldo y sitios de contingencia segundarios, han sido probadas por el autor, así como comprobadas por empresas que incorporaron estas tecnologías de manera exitosa. Un ejemplo en Costa Rica es el Hospital CIMA, que utilizó estas soluciones para dar alta disponibilidad a sus sistemas y ahorrar costos.

El diseño para pymes tiende a ser estandarizado con poca “tropicalización” por el tamaño pequeño o mediano de sus sistemas, y utiliza tecnologías comunes, como sistemas operativos Windows, bases de datos SQL Server, Sistemas de virtualización VMWare o Hyper-V. Esto permite una integración con mínimo o nada de interrupción, así como una ejecución en corto plazo, que normalmente no excede pocas semanas. Normalmente se presenta una prueba de concepto previo a la implementación, la cual emula el estado actual del cliente y presenta el resultado final esperado. También la misma tecnología permite reversar cualquier cambio de manera casi

instantánea, asegura así que la compañía no sufra algún perjuicio durante su implementación.

Punto de Vista Operativo

Entre los principales beneficios de la computación en la nube está que la misma puede ser accedida desde casi cualquier dispositivo y ubicación, siempre y cuando se tenga acceso al internet; por ello, si un desastre ocurriera, la información y los sistemas pueden ser accedidos desde cualquier lugar. Además, los sistemas de continuidad de negocio de hoy en día son mayormente automatizados, lo que implica una simplificación operativa en caso de que falle el sitio principal.

Para las pymes, por su baja capacidad en personal capacitado y certificado, se recomienda que subcontrate o tercerice a un proveedor de servicios en tecnología con especialización en el campo, esto facilita aún más todo proceso de integración, monitoreo y mejora continua sin aumentar los costos considerablemente. En caso de que la empresa quiera asumir el proceso operativo, existe gran cantidad de entrenamientos y la computación en la nube, que al ser altamente flexible y de bajo costo permite que los operadores hagan pruebas de concepto y simulaciones para rápidamente adquirir el conocimiento necesario en la operación.

Punto de Vista Económico

La flexibilidad de la computación en la nube, en donde se paga por uso de manera mensual, permite que los esquemas de recuperación de desastres se conviertan en un gasto operativo o OPEX, por ejemplo, el costo mensual de suscripción, reduciendo el riesgo y facilitando a las pymes la adquisición de este servicio. Ello a diferencia de hacerlo sin tecnologías de computación en nube o hosting, donde el gasto es capital o CAPEX, por ejemplo, la compra de hardware y software requerido por un mínimo normal de 3 años.

Se considera que al igual que como se describirá más adelante, la principal inversión se debe a la capacidad de cómputo, la cual únicamente generará cobro cuando exista un desastre. En relación con la recomendación de tercerizar los servicios de TI, los mismos también tienden a tener cobros no elevados y de igual manera mensuales, lo que permite adquirir la solución completa como un servicio, es decir, la tecnología, implementación y operación en una tarifa mensual a la medida.

Objetivos

Se utilizará la taxonomía cognitiva de Bloom, la misma organiza el aprendizaje en etapas aumentando su complejidad de manera gradual y facilitando que tanto los escritores como lectores inicien con conceptos básicos, se aumenta su complejidad sobre una base de información previa.

Objetivo General

Crear un modelo de recuperación contra desastres costo-efectivo para pymes utilizando computación en la nube.

Objetivos Específicos

- Identificar buenas prácticas en materia de recuperación de desastres.
- Definir ventajas de un sistema de recuperación contra desastres basado en computación en la nube.
- Diseñar una arquitectura referencial con su respectivo análisis de costo de los diferentes escenarios de recuperación.
- Generar guías de implementación de respaldo de información y replicación de sitio de datos.
- Producir un plan de pruebas de los diferentes escenarios de recuperación contra desastres.
- Formular computación en la nube como sitio primario para pymes.

Alcances y Limitaciones

Alcances

El siguiente documento presenta un modelo principalmente enfocado para aquellas pequeñas y medianas empresas que se encuentran en duda o necesidad de implementar un sistema de recuperación contra desastres costo-efectivo basado en la computación en la nube. Si bien la práctica no se limita a empresas medianas y pequeñas, se entiende que las empresas grandes por su complejidad requieren mayores configuraciones específicas, mientras que las pequeñas y medianas empresas son más estandarizadas, esto para traer simplificación en la integración, operación y predictibilidad de costos.

Este mismo modelo es funcional para cualquier vertical, ya sea educación, financiera, manufactura, tiendas o cualquier otra, enfocado al mercado latinoamericano, aun así, no limitado al mismo.

Limitaciones

El documento entregable es considerado una guía de entendimiento, así como de buenas prácticas, por lo que, aunque da una buena referencia, no es la única opción y puede integrarse con otras metodologías. También por la constante evolución de la tecnología, puede que guías y ejemplos mostrados en este documento varíen de la realidad posterior de las tecnologías. Considérese como limitante aquellas empresas que no pueden o quieren utilizar computación en la nube, ya sea por necesidad de datos ubicados en el país o cualquier otra limitante legal o técnica.

Estado de la Cuestión

Las pymes hoy en día mantienen sus equipos informáticos, como servidores, sistemas de almacenamiento y equipo de comunicaciones en pequeños cuartos de cómputo normalmente no adecuados, ya que son habitaciones con seguridad perimetral mínima, aires acondicionados de confort, los cuales no son precisos ni diseñados para operar 24x7. Se tiene a veces una única acometida eléctrica que no ofrece redundancia, falta de control de humedad y temperatura que puede llevar a los equipos a fallar, e incluso los cuartos son compartidos para labores de oficina o bodega. Además, hay casos más extremos en donde los equipos corren debajo de un escritorio y no debidamente instalados en un rack o gabinete especializado para el correcto soporte e instalación de estos equipos.

Estos cuartos de cómputo carecen de características de un centro de datos, como sistemas de alimentación redundantes en diferentes líneas de distribución eléctrica y de proveedores de electricidad diferente, áreas de enfriamiento de precisión redundantes, y baterías que protegen de las fluctuaciones eléctricas, estructura antisísmica. No cuentan con sistemas de supresión de incendio, normalmente por eliminación de oxígeno, además de una seguridad física y de acceso altamente restringida y controlada, entre muchas otras características.

Aunque existen diseños y guías para la construcción de centro de datos seguros, las pymes normalmente no están en capacidad económica de construir uno, mucho menos un segundo centro para uso secundario. Esto refuerza por qué las pymes no poseen un esquema de recuperación contra desastres, peor aún, la falta de un sitio adecuado aumenta la probabilidad de que el único sitio de producción falle de manera constante perdiendo productividad, imagen y demás.

Un segundo factor importante que limita la disponibilidad de los servicios son los equipos de cómputo. El costo de tener los sistemas más avanzados con múltiples tecnologías para evitar fallas, servidores robustos con fuentes de poder redundantes y sistemas operativos configurados de manera redundante,

sistemas de almacenamiento con redundancia en sus discos duros y diferentes mecanismos para prevenir fallos, sistemas de telecomunicaciones robustos, redundantes y seguros, entre muchas otras características, es muy elevado. Lo anterior normalmente lleva a las pymes a comprar equipos con características más básicas que no poseen todas las características necesarias para operar 24x/7 o bien susceptibles a fallos básicos.

Un tercer factor, igual de importante, es la capacidad tanto en cantidad de personal como su capacidad y experiencia. Por más seguro que sea el centro de datos y por más buenos que sean los equipos de cómputo, si desde su implementación hasta su operación continua no se tiene la suficiente cantidad de personal y con la habilidad adecuada, los equipos son más propensos a los fallos. Se necesita una cantidad de personal necesaria para operar equipos de cómputo, especialistas en servidores y sistemas operativos, especialistas en telecomunicaciones, especialistas en aplicaciones, especialistas en bases de datos, especialistas de seguridad, especialistas de almacenamientos, equipo de monitoreo 24x7 y equipo de innovación en tecnología. Fácilmente la cantidad de profesionales requeridos y sus capacidades técnicas hace que la operación adquiera un costo considerable, lo que fuerza muchas veces a las pymes a tener generalistas en vez de especialistas y en casos con operación 8x5.

Estos 3 factores, centro de datos, equipo cómputo avanzado y especialistas, conllevan a las empresas a tomar medidas de recuperación de desastres de básicas a inexistentes. Normalmente no tienen sistemas de archivo y respaldos robustos, mucho menos fuera de un sitio principal, además no tienen un centro de datos secundario para la replicación ni sistemas de monitoreo preventivo y reactivos adecuados.

Pymes

Las pequeñas y medianas empresas normalmente son categorizadas por dos factores, cantidad de empleados e ingresos. Una pequeña empresa normalmente tiene menos de 100 empleados y genera menos de USD$50 millones al año, y una mediana entre 100 y 999 empleados con ingresos entre USD$50 millones y USD$1000 millones, esto según en glosario de Gartner.

Marco Teórico o Conceptual

Del mainframe a la computación en la nube

Alrededor de los años 1970 se introdujo el Mainframe, eran equipos masivos que de manera centralizada procesaban datos, únicamente los tenían empresas e instituciones con altas capacidades económicas para poder adquirir dichos equipos. Se accedían a través de una terminal, la cual era una interface donde se introducía código y se esperaba que el sistema retornara un resultado; en sus tiempos, muchos usuarios hacían uso del mismo equipo y a pesar de su tamaño, sus capacidades eras minúsculas, aun así, más optimas que las tareas manuales.

Para los años 1980 se introdujo la computación personal, equipos mucho más reducidos en tamaño que permitían ejecutar aplicaciones sencillas de manera descentralizada, es decir cada usuario tenía su propia PC (computador personal) y ejecutaba sus propias aplicaciones según fuera necesario. Con la evolución de los mainframes y computación personal se introdujo la era de los servidores, los cuales son equipos de cómputo de alto rendimiento en donde, similar a los mainframes, se ejecutan tareas de procesamiento de manera centralizada, aunque a diferencia de su predecesor, eran mucho más reducidos en complejidad, costo y tamaño, lo que permitía que las empresas pudieran tener estos equipos de cómputo en áreas especiales denominadas centro de datos.

Estos centros de datos hospedaban múltiples servidores que procesaban centralizadamente información que era accedida a través de las computadoras personales mediante arquitecturas cliente/servidor, esto significa que los servidores procesaban y almacenaban la información que era accedida y manipulada desde múltiples computadores personales dentro de una red de comunicación interna de cada empresa. Con la introducción del internet, la cual es una red interconectada global, se empezó a hacer utilización de la Word Wide Web (www, por sus siglas en inglés) o red amplia global, la cual se accedía a través de un navegador web que permitía acceder contenido publicado por empresas alrededor del mundo, sin tener que estar conectado a

su red interna de comunicaciones. Esto permitía entonces que las personas pudieran acceder recursos tanto por la red interna como la red externa o internet.

Tanto en los servidores como computadores personales se ejecutan los sistemas operativos, los mismos son una capa de software que controla los distintos componentes de hardware del sistema como lo es la memoria, el almacenamiento en discos duros, los procesadores y comunicaciones, y permiten instalar sobre ellos aplicaciones con diferentes funcionalidades. La relación de un servidor físico con un sistema operativo único a pesar de que fue utilizado muchos años era ineficiente, dado que se necesitaban muchos servidores físicos para poder tener una arquitectura operativa funcional además de que no se aprovechaban los recursos al máximo. La virtualización fue la respuesta a dicho problema, la misma es una capa que permite a un hardware físico hospedar múltiples sistemas operativos de manera simultánea y asilada, se reduce así la cantidad de servidores y se da mejor utilización de ellos.

Dicha virtualización también trajo otros beneficios como la automatización, la cual permitía crear un servidor virtual en minutos y con mayor portabilidad al poder manipularse como un archivo desligado del hardware y sus componentes. La virtualización introdujo el concepto de definido por software, esto significa que las capas de procesamiento, almacenamiento y comunicación son administradas y controladas por software que corren independientes del hardware físico que las hospede. Esto permitió entonces que los equipos fueran cada vez más densos en capacidad hasta llegar a la híper convergencia, en donde múltiples equipos con capacidades de procesamiento, almacenamiento y comunicaciones, aunque separados interactúan como uno, con mayor escalabilidad en las aplicaciones con alta eficiencia en su uso.

Todo este proceso evolutivo nos ha llevado al concepto de computación en la nube, que son centros de datos masivos llenos de servidores ejecutando una capa de virtualización, la cual es administrada y definida por software que permite a las empresas utilizar los recursos que necesita, desde cualquier lugar.

Computación en la nube

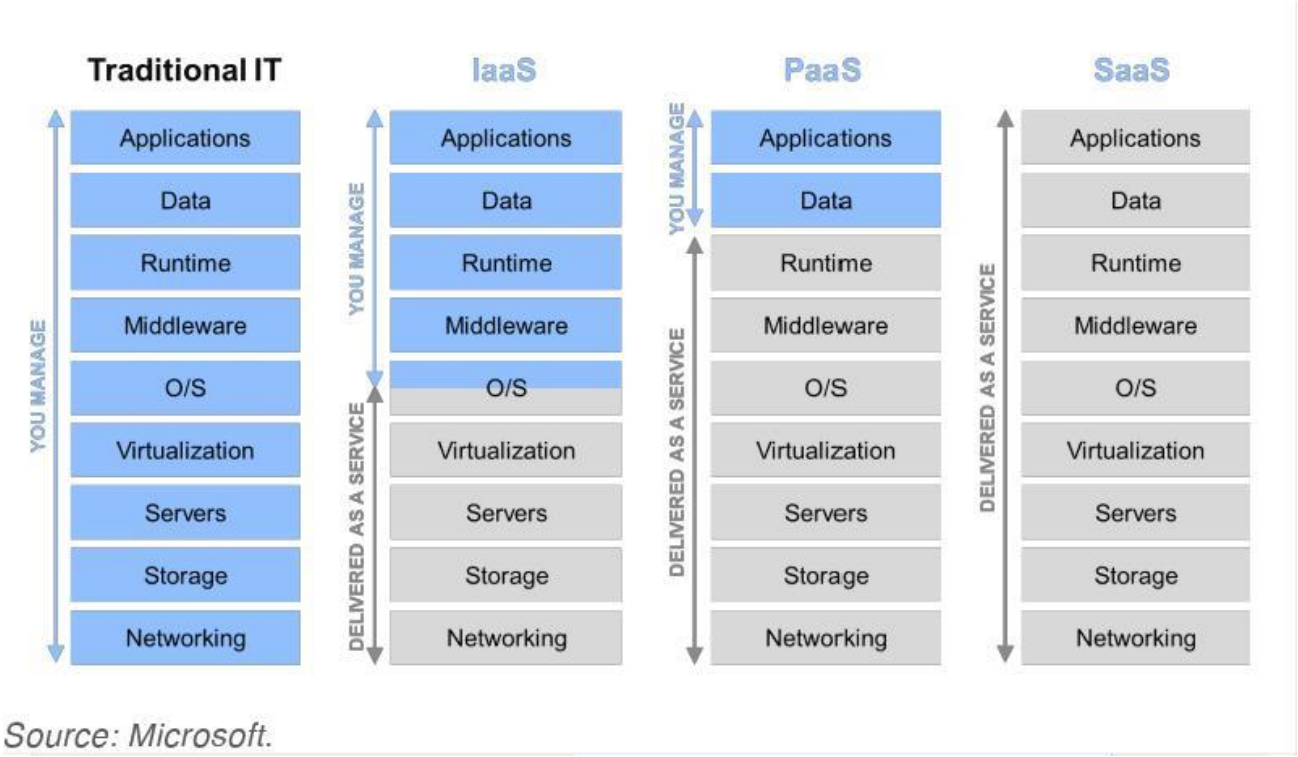
La computación en la nube posee múltiples ventajas, recursos virtualmente ilimitados, pago por uso, no requiere inversión capital o CAPEX, numerosas soluciones prediseñadas listas para ser utilizadas, accesible desde cualquier parte del mundo, así como seguridad aumentada e innovación sin precedente, entre otras. La computación en la nube, a pesar de que es muy amplia, se categoriza en 3 maneras.

En IaaS o infraestructura como servicio, por sus siglas en inglés, se contratan los servicios de centro de datos, servidores, almacenamiento, virtualización y comunicaciones como un servicio, es decir, el proveedor de servicios se encarga de toda la inversión equipos, así como su operación. Se deja entonces que la empresa se preocupe únicamente por el sistema operativo, datos y aplicaciones.

El modelo PaaS o plataforma como servicio agrega una capa adicional a manejar por el proveedor de servicios, en donde el mismo se encarga de tareas comunes como manejar el sistema operativo y su seguridad, respaldos y alta disponibilidad, así como la integración para simplificar el servicio. Deja entonces que el cliente final se enfoque más en el manejo de datos y la aplicación.

El tercer modelo es SaaS o software como un servicio donde el proveedor ofrece un producto final listo a ser consumido por el cliente, donde el cliente únicamente se preocupa por consumir el servicio y no de operar y mantener el mismo.

El siguiente cuadro ejemplifica de manera visual los diferentes modelos de computación en la nube.



Source: Microsoft.

Alta disponibilidad y continuidad de negocio

Los sistemas informáticos transformaron las industrias, permiten automatizar tareas manuales, realizar cálculos instantáneos, mejorar la colaboración y optimizan todo tipo de procesos, tanto internos y externos como procesos operativos y procesos de venta. Ya muchos productos y servicios se compran y/o consumen a través de plataformas digitales como páginas web y aplicaciones móviles, entre muchos otros, con sistemas informáticos ejecutándose 24/7 para dar soporte a los mismos. Esta alta dependencia de los sistemas informáticos crea la necesidad de que los mismos estén disponibles siempre, ya que, si un sitio web de compra no está disponible, la empresa no genera ingreso o si un servicio ofrecido no está disponible crea repercusiones tanto económicas como de satisfacción al usuario y de imagen.

La alta disponibilidad de sistemas informáticos se da mediante mecanismos de redundancia en todos sus componentes. La redundancia en TI

se entiende como la capacidad de que un servicio o solución siga operando aunque uno de sus componentes falle, desde redundancia en la arquitectura de servidores como múltiples fuentes de poder y múltiples discos duros en arquitecturas redundantes, hasta redundancia aplicativa como un “clúster” de base de datos que permite la misma resida en dos o más servidores en caso de que uno de ellos falle.

Esta alta disponibilidad permite entonces altos SLA (Service Level Agreement por sus siglas en inglés) que son una medida de cuánto tiempo está disponible un servicio. Idealmente los servicios deberían tener un SLA no menor a 99.9%, el cual significa que los servicios no deben estar fuera de línea por más de 43 minutos mensuales o 8 horas y 45 minutos anuales.

Evidentemente a mayor criticidad de la aplicación el SLA requerido será aún mayor, igualmente si el servicio no es crítico un SLA más bajo es aceptable. Dado que la redundancia de componentes se da de manera local, es decir, todos los equipos y suministros están localizados en un mismo centro de datos, se debe introducir el concepto de recuperación contra desastres. Esto significa que debe existir una contingencia fuera del centro de datos primario en caso de que el mismo falle ya sea por desastres naturales, desastres tecnológicos o labores humanas como mantenimientos de tecnologías y propias de los centros de datos.

Respaldo, archivado y sitio de datos secundario

El principal activo informático de una empresa es la información, los equipos lo que realizan es procesamiento, almacenamiento y comunicación, de esta información y las aplicaciones nos permiten manipularla y presentarla de una manera que haga sentido al usuario. Como tal, que la información esté siempre disponible, en cualquier situación, es una tarea de suma importancia.

Los respaldos nos permiten tener una copia de seguridad de la información, ya sean bases de datos, archivos e imágenes o copias completas de servidores operacionales. Los respaldos son esenciales para casos de

pérdida de datos, nos permiten tener un mecanismo para recuperar la información sin embargo no están limitados a una falla, pongamos el caso hipotético de qué pasa si un usuario autorizado elimina información de una base de datos por error. Aunque la aplicación esté 100% funcional, la misma no podría retornar la información eliminada.

Los respaldos tienen la característica de que normalmente son almacenados en sistemas de rápido acceso como discos duros, para tener la información a primera mano en caso de ser necesitada. Un sistema de respaldo normalmente está compuesto por un software que gestiona y realiza los respaldos, así como un sistema de almacenamiento centralizado, a diferencia de los respaldos que son copias de rápido acceso operacional normalmente no mayores a 6 meses de datos. El archivado es un proceso similar pero normalmente es donde se guardan los históricos por más años; en su mayoría son raramente utilizados, por lo que se almacenan en unidades de cinta que son secuenciales y lentas, además de que son más costo-efectivos que los discos duros.

Los archivos en el párrafo anterior permiten a una empresa desde cumplir con normas y leyes en la manutención de datos, hasta la capacidad de que una empresa pueda recuperar o validar información guardada a lo largo del tiempo. Es esencial que en la continuidad de negocio se contemple un sitio alterno, ya que si guardamos los respaldos en un mismo sitio donde están los equipos de producción y este es afectado por un desastre natural, actos vandálicos como robo o bien desconocimiento en la manipulación de datos del personal, la data no estará disponible. Este escenario incluso puede llevar a pérdidas importantes en una empresa, ya que la misma no podría recuperarse si se destruye su única copia de datos. Un ejemplo sería perder la lista de facturas por cobrar en una empresa en caso de que la misma sea eliminada por error.

Ahora bien, un sitio alterno no es únicamente para almacenaje de datos, según las necesidades de una empresa, la misma puede necesitar un sitio secundario para procesar datos, es aquí donde introducimos técnicas para replicación entre centro de datos, en donde si un centro de datos no está

disponible se activan mecanismos para que los sistemas funcionen desde un centro de datos secundario. Si bien un respaldo nos permitirá recuperarnos en un centro de datos secundario, el proceso de recuperación puede tomar días, semanas y hasta meses, mientras que la replicación entre centros de datos de procesamiento puede ser de horas.

Finalmente, esto ayuda a una empresa a cumplir su RTO (Recovery Time Objective), es decir el tiempo máximo que la misma puede estar fuera de línea en caso de una falla. La velocidad a que se sincronizan los datos determina también el RPO (Recovery Point Objective), que indica cuánta data se está dispuesta a perder para recuperarse en el tiempo objetivo o RTO.

Buenas prácticas en materia de recuperación de desastres

Las buenas prácticas en recuperación de desastres pueden variar según el tamaño de la empresa, el modelo de negocio, así como la dependencia del uso de tecnología. Una cadena de gimnasios puede estar sin sistema de punto de venta por días, sencillamente porque recibe pocas transacciones diarias y en su mayoría el cliente es recurrente, por lo que es más fácil cobrarles un día posterior. Una gasolinera recibe múltiples clientes por hora y un cobro posterior no es viable, por lo que su sistema de punto de ventas es más crítico. Aun así, se enlistarán las consideraciones que se recomiendan se validen indiferentemente del tamaño, pero se debe tener claro que para una empresa una recomendación podrá tener más peso que otra.

Identificar y priorizar aplicaciones críticas

Un análisis de impacto nos permite determinar cuáles son los sistemas que generan la mayor cantidad de pérdidas, ya sea de productividad de empleados, económicas, de imagen o bien una combinación de las anteriores. Si bien lo ideal es que todos los sistemas sean altamente disponibles y tengan contingencia, no siempre es posible protegerlos todos a la vez, ya sea por su costo o dificultad en su implementación. Identificar los sistemas más críticos y sus dependencias es clave en la recuperación contra desastres.

Crear un plan de implementación controlado

Luego de lograr identificar las prioridades es importante planear correctamente, así como implementar las tecnologías de recuperación contra desastre. Lo que menos se quiere es implementar un sistema de contingencia que genere fallas durante su implementación.

Ejecutar pruebas periódicas

Después de implementar un sistema de contingencia es importante comprobar su funcionalidad de manera periódica, esto nos asegura que realmente el sistema funciona y podemos depender de él. Restaurar datos críticos de un respaldo, o bien activar un sitio de secundario nos ayuda a que el equipo esté constantemente entrenado en caso de un suceso permitiendo que reaccionen correctamente ante una eventualidad.

Ajustar correctamente por cambios

Los sistemas cambian, ya sea de versión, un nuevo sistema se instala o incluso la prioridad de una aplicación puede variar con el tiempo. Es importante que todo cambio sea contemplado y se hagan los ajustes necesarios para asegurar disponibilidad de los servicios.

Proyectar crecimiento

Es natural que los nuevos sistemas requieran más recursos de cómputo, que los respaldos crezcan en el tiempo e idealmente la información aumente según crezca el negocio. Se debe proyectar el suficiente crecimiento en capacidades de los sistemas para asegurar que no exista escasez de recursos. Si proyectamos incorrectamente, una aplicación critica puede no tener los suficientes recursos para que trabaje de manera fluida y puede, aunque esté encendida, que no sea funcional. Otro escenario es que nos quedemos sin espacio donde almacenar los últimos respaldos, entonces en un caso de un desastre no tendremos la información más actualizada a disposición.

Usar un standard como guía, ejemplo ISO/IEC 22301:27031

Los estándares nos ayudan a seguir una línea ya probada de recomendaciones y buenas prácticas a seguir, además dan buena reputación e incluso puede llegar a ser una ventaja competitiva considerable a nivel o incluso un requerimiento de cumplimiento. ISO 22301 es un buen ejemplo, el mismo cubre la continuidad de negocio como un todo mientras que el ISO 27031 se enfoca en la recuperación de negocio más como un aspecto técnico. Tengamos claro que el ISO nos dice qué hacer, ejemplo identificación de riesgos, políticas y procedimientos, pero no nos dice cómo hacerlo, ejemplo usar alguna tecnología específica.

Reducir el error humano, automatización

Idealmente se debe depender lo menos posible de personas para poder ejecutar un plan recuperación, no queremos tener un sistema maravilloso que falle el día que el empleado estrella esté ausente. La automatización es clave para la detección y activación de un plan, además que los sistemas no se estresan en una situación de desastre perdiendo perspectiva, sino que sencillamente ejecutan lo que les fue programado.

Asignar responsables y capacitar

A la hora de un fallo, lo peor que puede pasar es que nadie sepa a quién acudir o que no exista un nivel de entrenamiento adecuado para accionar, como tal saber quiénes son los responsables por las aplicaciones o bien un proceso de escalación y notificación es importante para que los empleados sepan qué hacer. Es de igual importancia que las personas estén capacitadas según su función, ya sea algo básico como un usuario final hasta algo avanzado como el responsable, esta capacitación debe ser constante para que no se olvide o que un nuevo empleado lo desconozca.

Buscar apoyo

En su mayoría, las empresas se dedican a su propio negocio no relacionado con la venta de tecnología, por lo que los sistemas no es su fuerte. Existen muchas empresas que sí son expertos en el área de recuperación de sistemas que pueden asesorar, implementar e incluso ser responsables por la continuidad de negocio de la empresa. Se debe buscar apoyo en ellos, lo que reduce el tiempo de implementación, tiempos de reacción y costos, dado que se les paga por el servicio y ellos son los que mantienen el personal entrenado y disponible, entre otros.

Ventajas de un sistema de recuperación contra desastres basado en computación en la nube

La computación en la nube ofrece una innumerable cantidad de beneficios sobre las tecnologías tradicionales; las capacidades masivas de cómputo, las economías a escala, la especialización de los proveedores de tecnología, la constante innovación, el énfasis en ciberseguridad y las nuevas tecnologías, entre muchas otras. Estos beneficios son muy atractivos, y bien se pueden traducir a escenarios específicos para recuperación contra desastre.

Bajo costo

Este es claramente uno de los beneficios más importantes, principalmente para las pymes que son sensibles a gastos importantes. La computación en la nube incluye todo el costo de mantener, operar y asegurar un centro de datos, gastos eléctricos y de enfriamiento, incluye los costos de hardware físico, los servidores, equipo de comunicación, equipos de almacenamiento, virtualización y portales administrativos, entre muchos otros. La computación en la nube nos permite poder comprar los componentes que necesitamos y pagar solo por su uso, no se tiene desperdicio de recursos y se paga mes a mes como una factura eléctrica. Los centros de computación en la nube, por su escala masiva de miles y miles de servidores, permiten que los precios sean menores a operarlo internamente.

Rápido de implementar

Dado que los recursos siempre están disponibles en la nube, los mismos se pueden implementar de manera inmediata, lo único que se debe hacer es tener la suscripción disponible y se provisionan los recursos. Esto acelera rápidamente cualquier implementación, ya que no se requiere compra de equipos y que los mismos sean entregados, luego instalados y configurados para poder inicia un proyecto de recuperación contra desastres. Además, las

tecnologías de computación en la nube se integran fácilmente, muchas veces de manera nativa, a las aplicaciones tradicionales, por lo que llevar una implementación a cabo es tema de horas.

Falle rápido y barato

Un gran beneficio de la computación en la nube es que se pueden probar las cosas rápidamente y a bajo precio, al no tener que prepagar o comprar ningún equipo; sencillamente habilitamos los recursos que necesitamos y si no funcionan los apagamos y se dejan de cobrar. Esto permite gran flexibilidad y reduce el riesgo de un gasto económico grande innecesario.

Fácil de probar

Las tecnologías de recuperación de desastres tienen mecanismos de pruebas que pueden activarse en minutos, podemos fácilmente recuperar un archivo de un respaldo o bien hacer pruebas del data-center secundario incluso en paralelo al primario y sin afectarlo. Esto es muy importante para asegurar la correcta funcionalidad de los sistemas, así como cumplir con auditorías internas y/o externas de ser necesario.

Escalable

Dado que la computación en la nube ofrece virtualmente ilimitada cantidad de recursos, podemos fácilmente asignar más recursos de cualquier tipo cuando sea necesario. Esto permite una expansión inmediata y asegura así siempre la cantidad de recursos requeridos para el crecimiento natural de la empresa, así como de nuevos sistemas.

Automatización

La computación en la nube permite todo tipo de automatización, en la creación de recursos, así como en la ejecución de una acción según pase un evento. Esto reduce el error humano, así como el tiempo de reacción.

Imaginemos que, si un centro de datos falla, el mismo sistema automáticamente detecta que el mismo dejó de funcionar y se encarga de encender su servicio de contingencia sin intervención.

Arquitectura referencial y análisis de costo de los diferentes escenarios de recuperación

Es importante recalcar que la recuperación contra desastres usando computación es de fácil uso, como tal su entendimiento debe ser simple. Para esto se crean diagramas sencillos, así como sus cotizaciones fáciles de interpretar. Mantendremos el enfoque en los dos escenarios que hemos venido trabajando, estos son respaldos, así como un sitio secundario.

Arquitectura de respaldos híbrido

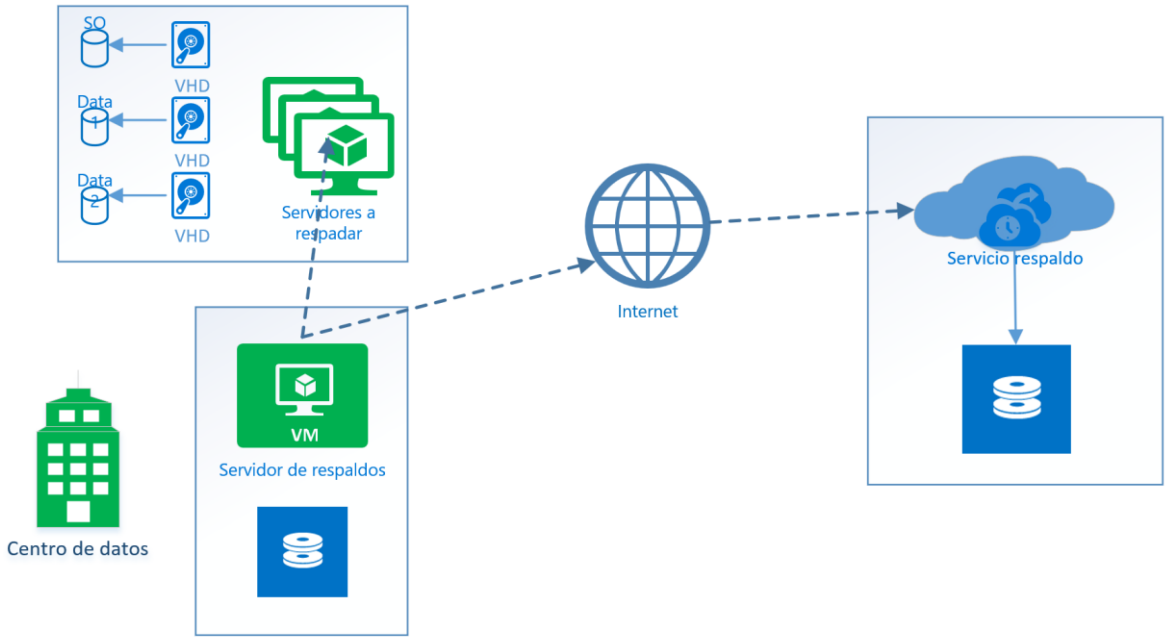
Recordemos que respaldo híbrido es crear y mantener un respaldo local en el centro de datos por un corto periodo de tiempo, normalmente días, mientras que las copias a más largo plazo se envían a la nube mediante el internet.

El centro de datos local, normalmente en las oficinas del cliente, está compuesto por una serie de equipos como servidores de cómputo, equipo de almacenamiento, equipo de comunicaciones, entre otros. Sobre los servidores físicos se instala un software de virtualización que nos permite tener múltiples máquinas virtuales en donde se hospedan los sistemas operativos con las aplicaciones propias de la empresa, a estos los llamaremos servidores a respaldar. Contiguo a estos servidores instalaremos un servidor de respaldos, el cual tendrá un software especializado para realizar dicha tarea, este servidor se conectará con los equipos a respaldar mediante un agente que se instalará tanto dentro del sistema operativo, así como en el software de virtualización.

Esto permitirá que el servidor de respaldos pueda acceder a la información de las aplicaciones, así como la capacidad de crear una copia completa de los discos duros virtuales, o VHD por sus siglas en inglés. El servidor de respaldos ejecuta tareas programadas que respaldarán la información en sus discos duros locales para luego transmitirlas por internet hacia la bóveda de datos que existe en la nube. Con la información en la nube se mantendrá vigente hasta que el respaldo cumpla el vencimiento al que fue programado. De manera invertida, restaurar un respaldo en la nube requiere

del servidor de respaldos para que pueda descargar la información de la bóveda en la nube hacia el servidor de respaldos local por internet, para su posterior puesta en producción.

Podemos apreciar en el siguiente diagrama la configuración anteriormente descrita.



Análisis de costo para respaldos

Para efectos de poder dar un orden de magnitud, se calcula el costo de respaldar 5 servidores (también llamado instancias de respaldo) con una cantidad de 200GB de información por servidor. El costo del servicio sería de $74 al mes, incluye las licencias para los 5 servidores, incluye licencia del software de respaldos, así como los 1000GB de las 5 instancias sumadas. Dado que la computación en la nube cobra por consumo real, los $74 asumen que los 1000GB están utilizados. Un beneficio adicional de este servicio de respaldos es que posee compresión de datos, es decir, reduce la cantidad de almacenamiento utilizado mediante la compresión de información; se reduce entonces el consumo de GB en la nube, lo que se traduce en reducción de todos.

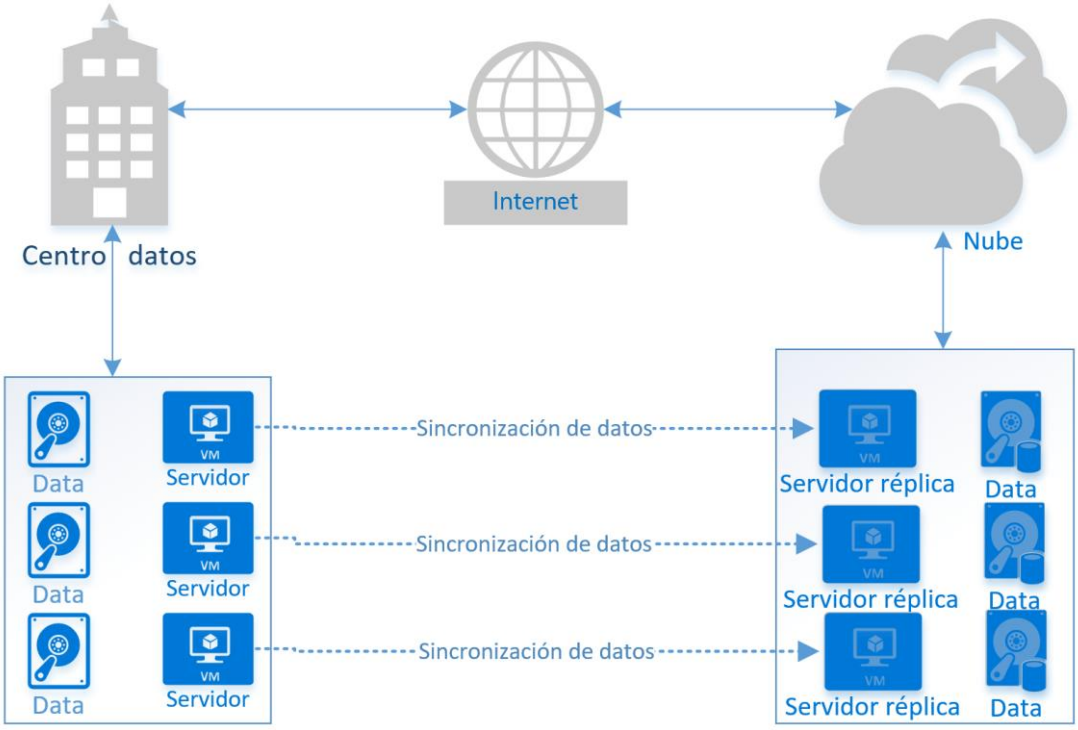
Microsoft Azure, estimacion de costos		
Su presupuesto		
Tipo de servicio	Descripcion	Costo estimado mensual
Respaldo	5 instancias, 200GB x instancia (1000GB total) LRS	$74.00
Estimado creado el 6/4/2018		

Arquitectura de sitio alterno

Al igual que el escenario de respaldos, el centro de datos local, normalmente en las oficinas del cliente, está compuesto por una serie de equipos como servidores de cómputo, equipo de almacenamiento y equipo de comunicaciones, entre otros. Sobre los servidores físicos se instala un software de virtualización que nos permite tener múltiples máquinas virtuales en donde se hospedan los sistemas operativos con las aplicaciones y datos propios de la empresa.

En el esquema de recuperación contra desastres, vamos a replicar las máquinas virtuales contra la nube vía internet creando así un servidor réplica. La réplica requiere una sincronización inicial de datos, que es equivalente al tamaño completo de la máquina virtual para luego nada más hacer réplicas incrementales de los datos. La velocidad de dicha replicación dependerá del enlace de internet, por lo que se recomienda que sea lo suficientemente rápido para acelerar el proceso de implementación.

Este proceso de replicación se hace en vivo, es decir, no requiere de apagar los servidores originales por lo que no afecta la operación continua de la empresa. Para tecnologías de virtualización VMWare se requiere de VMWare VCenter, el cual es el software que administra los servidores de virtualización y se requiere instalar una máquina virtual con el servidor de configuración a Azure, este es un servidor que se encarga la comunicación con Azure. Para virtualización Hyper-V no se requiere del servidor de configuración, ya que el mismo se logra comunicar de manera nativa con la nube de Azure.



Análisis de costo para sitio alterno

Para poder hacer un cálculo de sitio alterno, primero debemos entender los 4 principales componentes y cómo los mismos se consumen.

- Licencias de orquestación.
    - Esta licencia, que tiene un costo fijo por servidor a replicar, es la que se encarga de toda la orquestación en la replicación de la máquina virtual, dirige hacia dónde deben replicar los datos y cada cuánto se deben estar sincronizando. Preconfigura el servidor réplica y monitorea el servidor origen, preconfigura las comunicaciones además de que es el que permite iniciar el proceso de levantamiento del sitio secundario en el orden adecuado de manera automática. Esta licencia es el cerebro de la operación.

- Volúmenes de datos
    - Las máquinas virtuales son replicadas a una bóveda de replicación, la misma se réplica en forma de discos duros virtuales. El cobro de estos volúmenes es proporcional al tamaño utilizado, es decir se cobra por GB de almacenamiento requerido, por lo que su costo es variable según el ambiente origen.
- Cómputo
    - Idealmente la máquina virtual réplica posee las mismas características de recursos que la máquina virtual origen en tamaño de memoria RAM, así como de procesadores, sin embargo, la misma solo se enciende por una prueba o por un fallo. Como tal, si no existe encendido del sitio secundario no existiría costo de cómputo, ya que el mismo solo se cobra si se usa, un gran beneficio de la computación en la nube.
- Conectividad
    - Conexión: Ya por el servidor réplica estar en la nube se requiere algún método de conexión al mismo, ya sea por una IP Pública o por una conexión virtual privada. Estas las podemos tener

siempre funcionando, lo cual reduce el tiempo de recuperación porque están listas de antemano, pero aumenta el costo por el consumo ya que tener la conexión VPN activa genera un costo por hora.

- Transferencia: Las nubes públicas cobran por la descarga de datos, no por la subida. Al encender el centro de datos en Azure y conectarnos a los servidores se generan transferencia de datos bidireccionales, la nube únicamente cobra el dato saliendo de la nube hacia el usuario. Este gasto suele siempre ser muy pequeño, incluso descartable si el sitio secundario tiene muy poco uso.

Ya que entendemos mejor los 4 componentes, la cotización incluye:

- ✓ 5 licencias de orquestación.
- ✓ 5 discos duros de 128GB (640GB totales).
- ✓ 5 servidores de 4 procesadores y 8GB en RAM encendidos por 24 horas al mes con sistema operativo Windows.
- ✓ Conexión de enlace VPN por 24 horas y una transferencia de Datos de 50GB.
- ✓ 2 direcciones de IP Pública.

Esto entonces nos da un costo mensual de USD$200.91, como se muestra en la siguiente tabla.

Microsoft Azure, estimación de costos		
Su presupuesto		
Tipo de servicio	Descripción	Costo estimado mensual
Licencia ASR	5 instancias a Azure, 5 discos S10 (128GB)	$154.44
Computo	5 servidores A4 v2 (4 vCPU; 8 GB de RAM) x 24 horas; Sistema operativo Windows	$34.32
VPN	Puertas de enlace de VPN, nivel VpnGw1, 24 horas de uso, Transferencias de datos 50GB	$6.31
IP Pública	2 direcciones IP Publica estáticas	$5.84
		$200.91
Estimado creado el 6/4/2018 de https://azure.microsoft.com/es-es/pricing/calculator/		

En resumen, un ambiente de respaldo y recuperación de desastres para 5 servidores suman $275 al mes, un monto muy accesible para una mediana e incluso una pequeña empresa en busca de asegura su continuidad de negocio. Dicho costo es ínfimo comparándolo con la compra, operación y mantenimiento de un sitio secundario con todos sus equipos y software equivalente al sitio primario, además la computación no requeriría de un costo capital que sí requiere un sitio secundario, lo que reduce increíblemente la barrera de entrada.

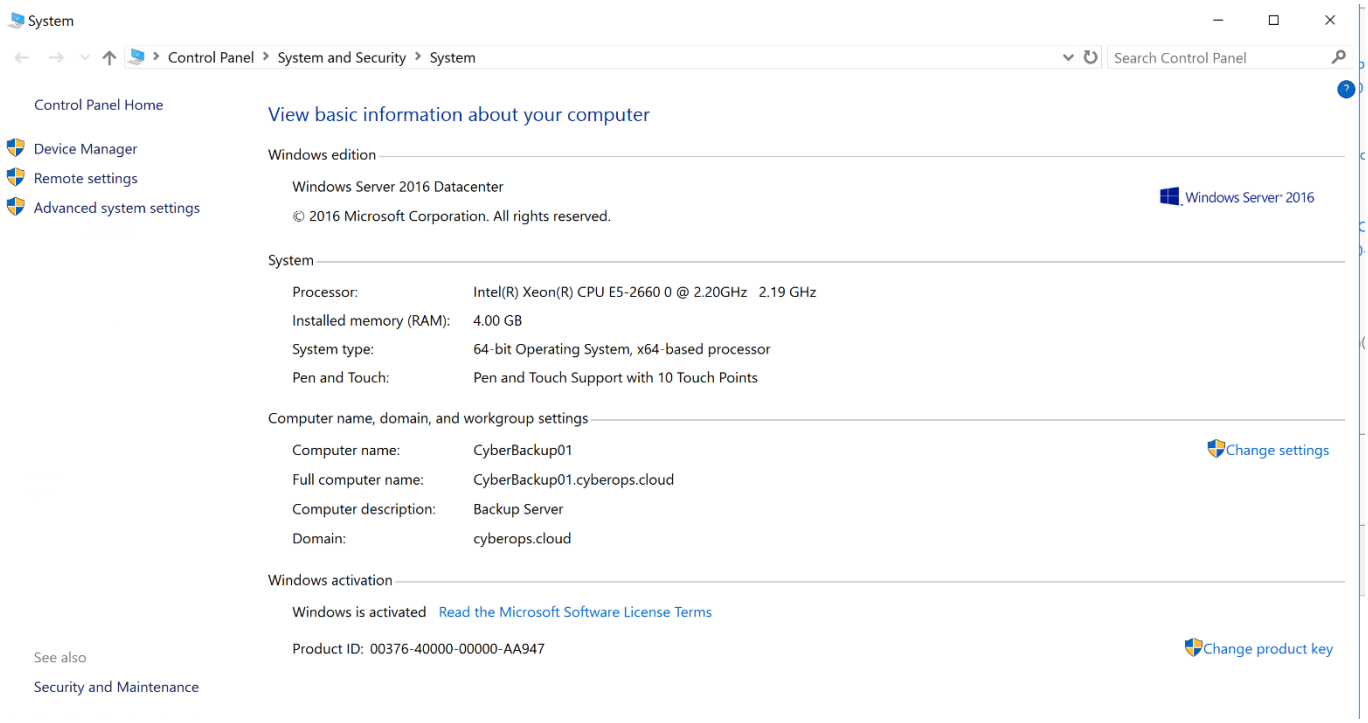
Guía de Implementación

En este capítulo se hará la configuración e instalación de los componentes necesarios para hacer respaldos en la nube, así como replicación de máquinas virtuales. Si bien el ambiente real del cliente puede variar respecto a su configuración y tecnologías actuales, se presentará un escenario base para entender bien el funcionamiento. Esta guía no pretende ser exhaustiva en todos los escenarios, sino que busca dar una explicación fundamental de cómo funciona, suficiente para entender el proceso de implementación y poder replicarse.

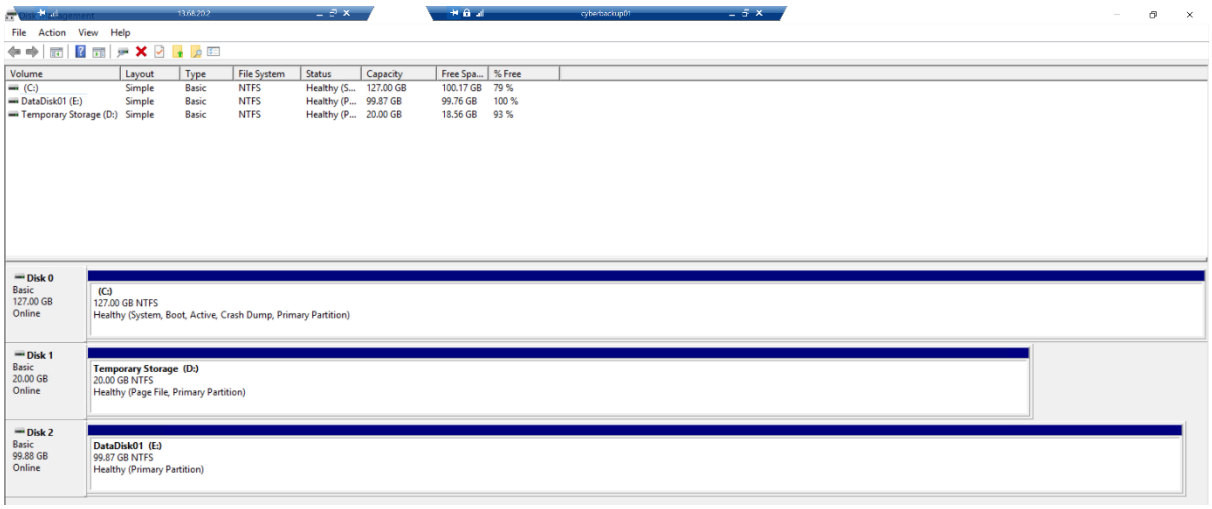
Instalación Servidor de respaldo y archivado

Para hacer una estrategia de respaldo híbrida es necesario instalar un servidor con Windows Server, preferiblemente la última versión disponible, en la misma red y localidad de los servidores actuales. Dado que hoy en día se utiliza mucho la virtualización, este servidor se recomienda sea una máquina virtual para optimizar los recursos del hardware además de portabilidad, aunque el mismo puede ejecutarse sobre un servidor físico.

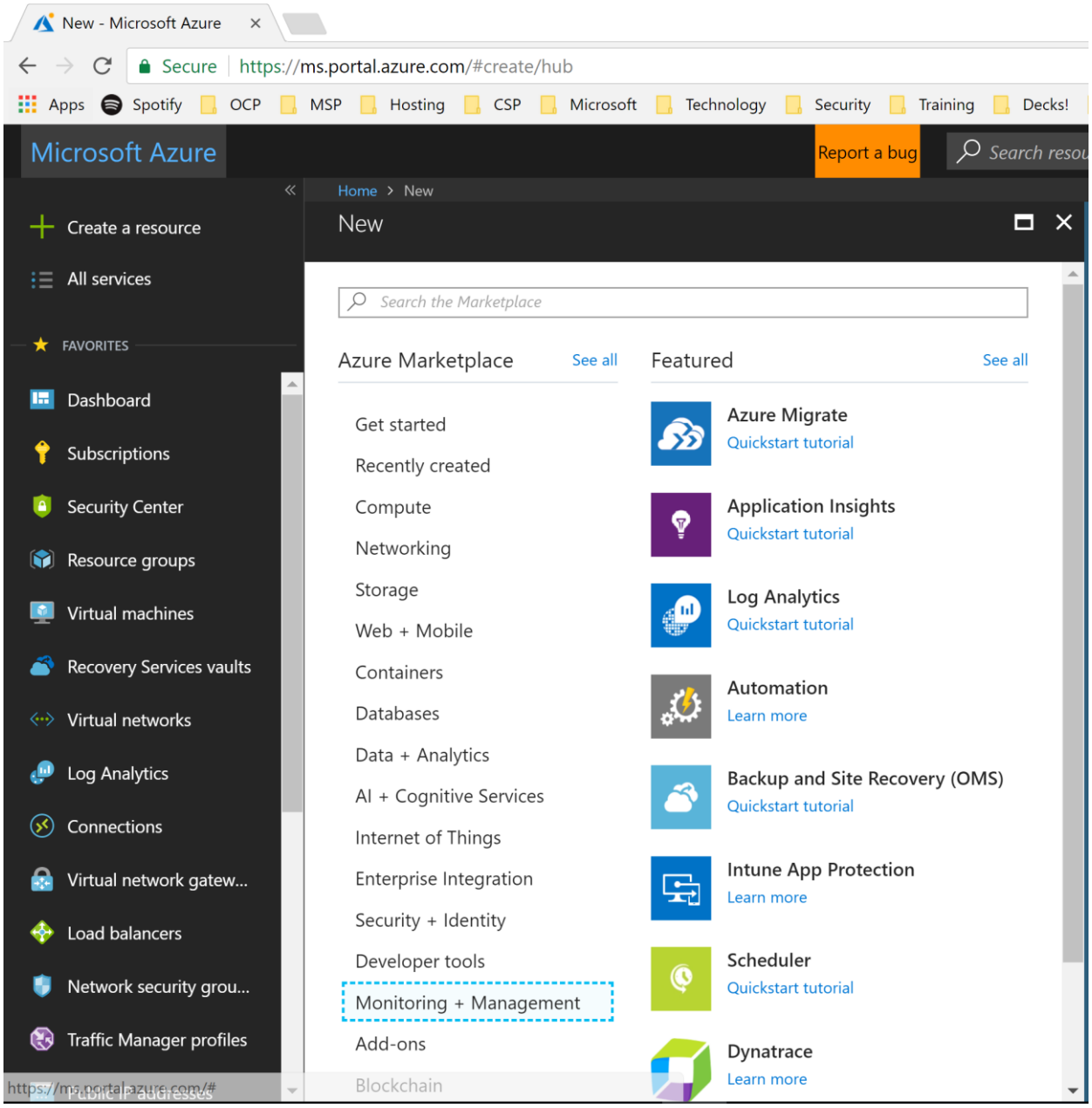
Adicionalmente, de ser ejecutado sobre un servidor físico, debe ser parte de los servicios de dominio de la empresa, (dominio directorio activo) como requisito de la herramienta de instalación de respaldos llamada “Azure Backup Server”, de igual manera se recomienda el mismo entre en las políticas normales de la empresa de actualización, seguridad y monitoreo, entre otras. De no existir un controlador de dominio como alternativa, se puede utilizar otra herramienta de respaldo Netbackup de Symantec o DataProtector de HPE.



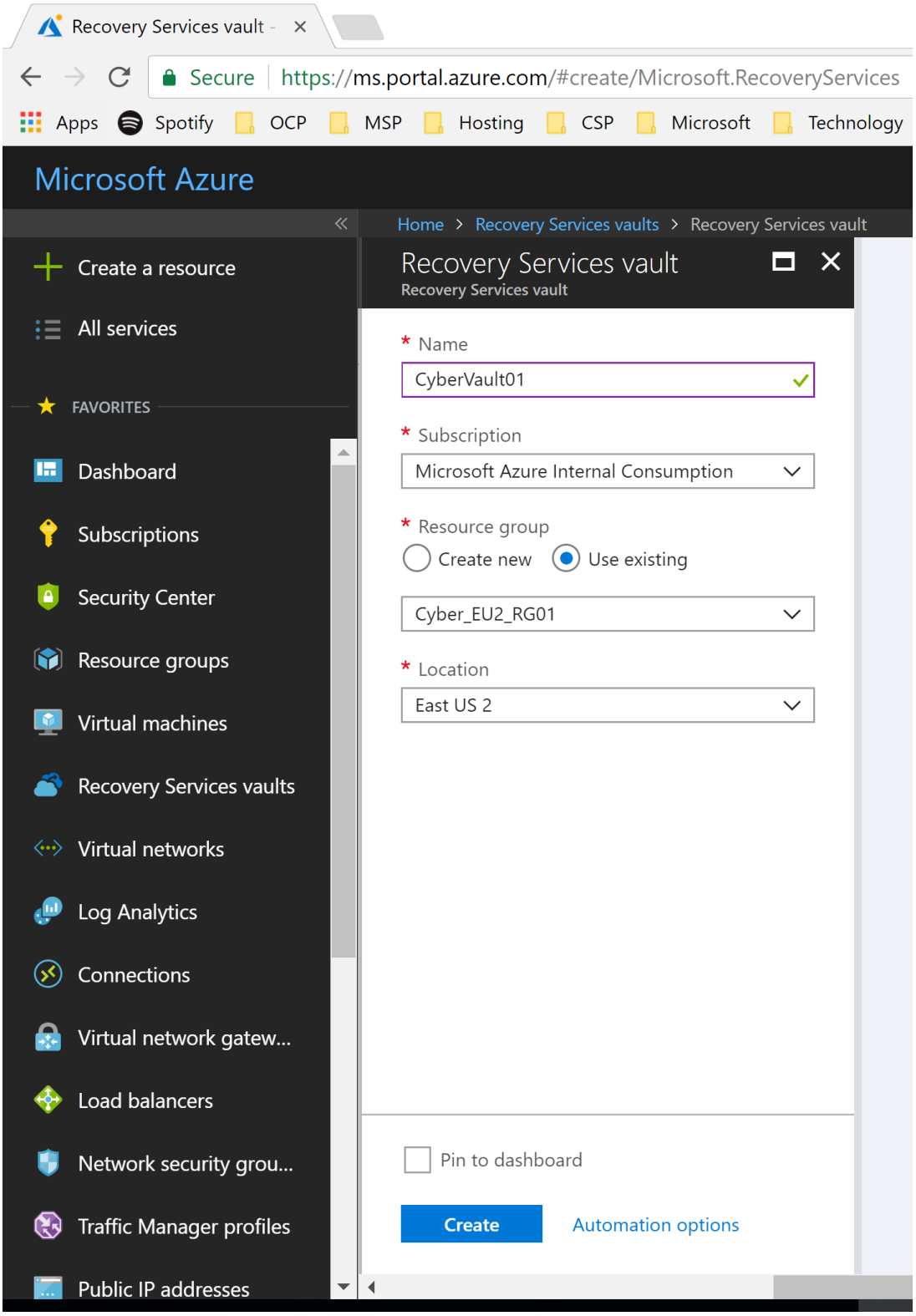
Como el servidor es de respaldo híbrido, es decir, que mantendrá una copia de datos en disco local por un periodo de tiempo corto normalmente en el rango de días, el mismo debe poseer un volumen de datos lo suficientemente grande para poder mantener la cantidad de información a respaldar con la retención escogida. A recomendación del autor, debería tener 2 veces la capacidad de información a respaldar con retención de los datos entre 7 a 15 días. Es decir, si necesitáramos respaldar 1 Terabyte (TB) de información se recomienda que el mismo tenga una partición de datos de por menos 2 TB. Para nuestra guía, asignamos un disco llamado DataDisk01.



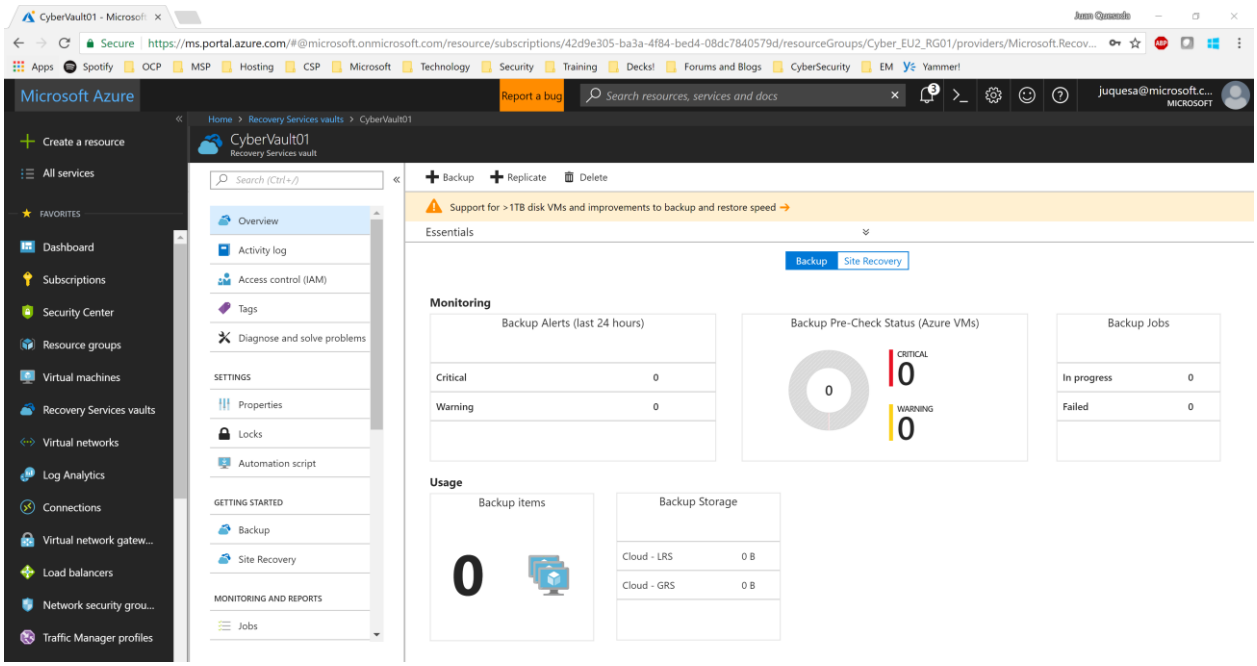
Luego de tener listo el servidor, debemos crear una bóveda de respaldos en la nube de Azure. Para esto debemos tener una suscripción disponible, ya sea comprada por la página web o algún socio vendedor, como por ejemplo los proveedores de soluciones Cloud (CSP por sus siglas en inglés). Esta bóveda es donde se almacenarán los datos de manera encriptada. Para crear la bóveda, navegamos dentro de https://portal.azure.com en esquina izquierda superior buscamos “create a resource”, navegamos a “Monitoring + Management” y damos click en backup and site recovery.



Completamos la información solicitada, le ponemos un nombre a la bóveda, seleccionamos la suscripción, así como el centro de datos a usar.



Pocos segundos después la bóveda estará creada, se debe mirar como en la imagen.



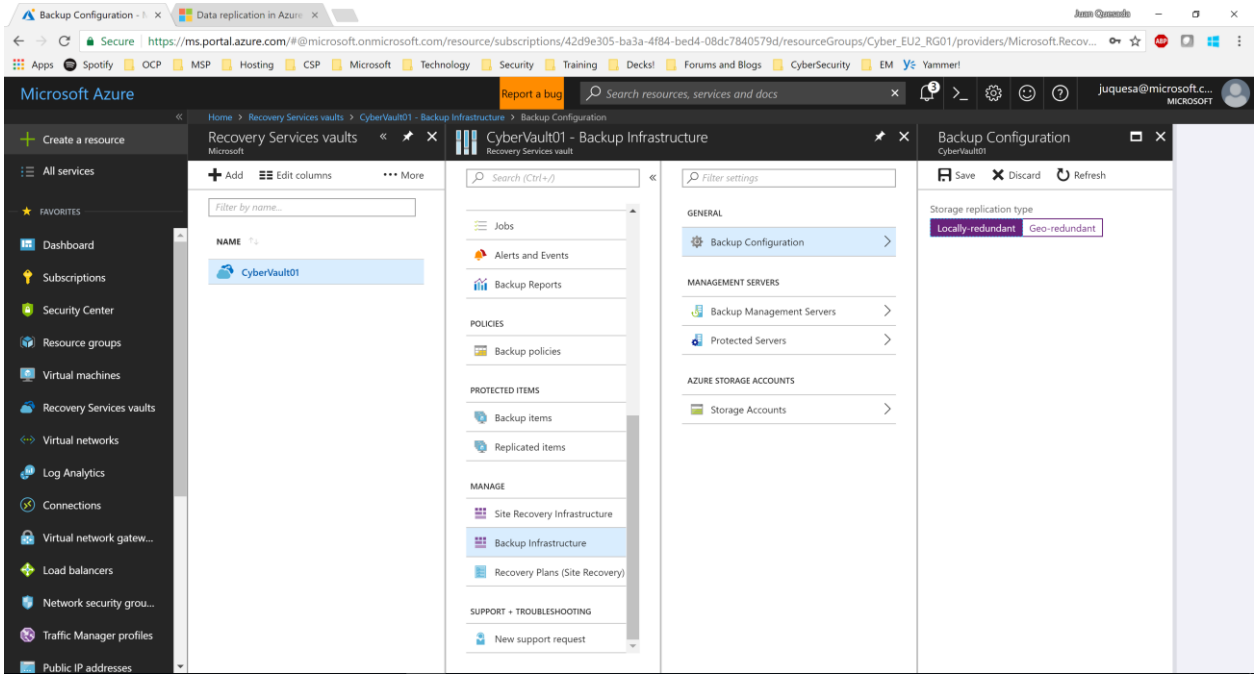
El primer paso que debemos seguir para respaldos es escoger el tipo de almacenamiento que queremos usar, en backup infraestructure, backup configuration.

<u>Tenemos dos opciones:</u>

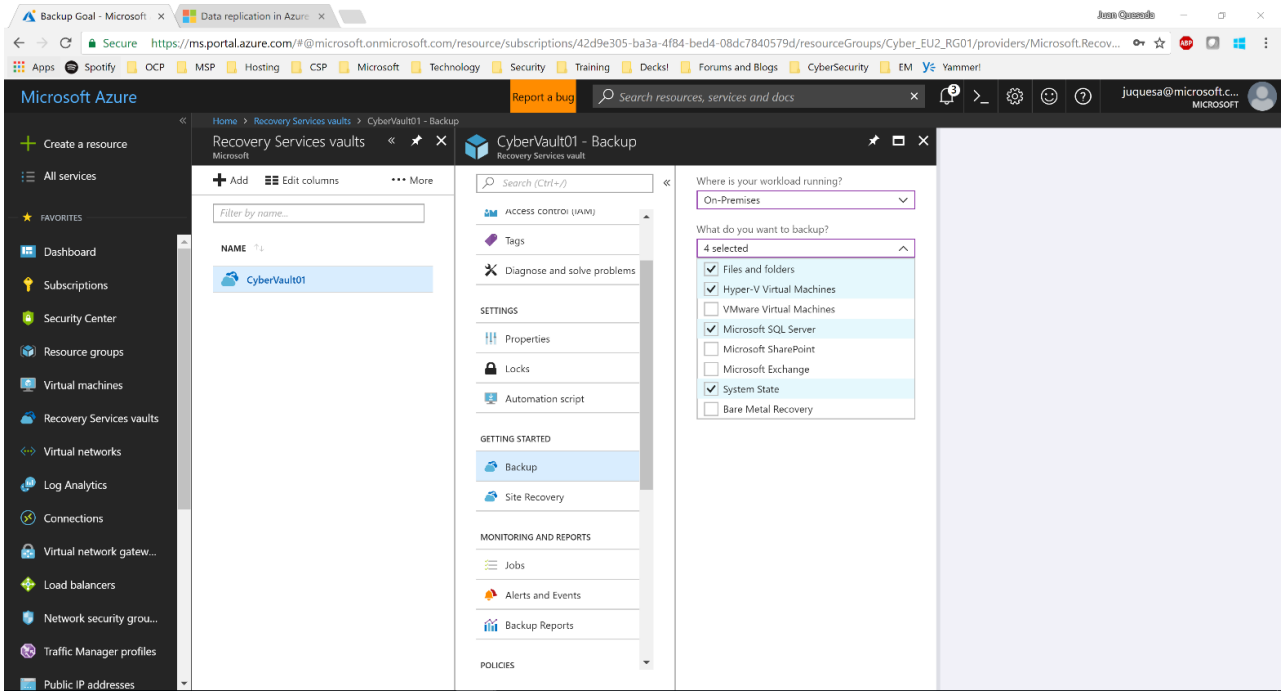
LRS (Locally Redundant Storage) o almacenamiento localmente redundante, que significa que el almacenamiento tendrá 3 copias dentro del mismo centro de datos. Esto ofrece un SLA de 99.999999999% (11 9‘s).

GRS (Geo Redundant Storage) o almacenamiento geo redundante, que significa que el almacenamiento tendrá 3 copias dentro de un mismo centro de datos y otras 3 copias en otro datacenter geográficamente a más de 160km de distancia. Esto ofrece un SLA de 99.99999999999999% (16 9’s). Esta cuesta el doble del anterior, al duplicar la información almacenada.

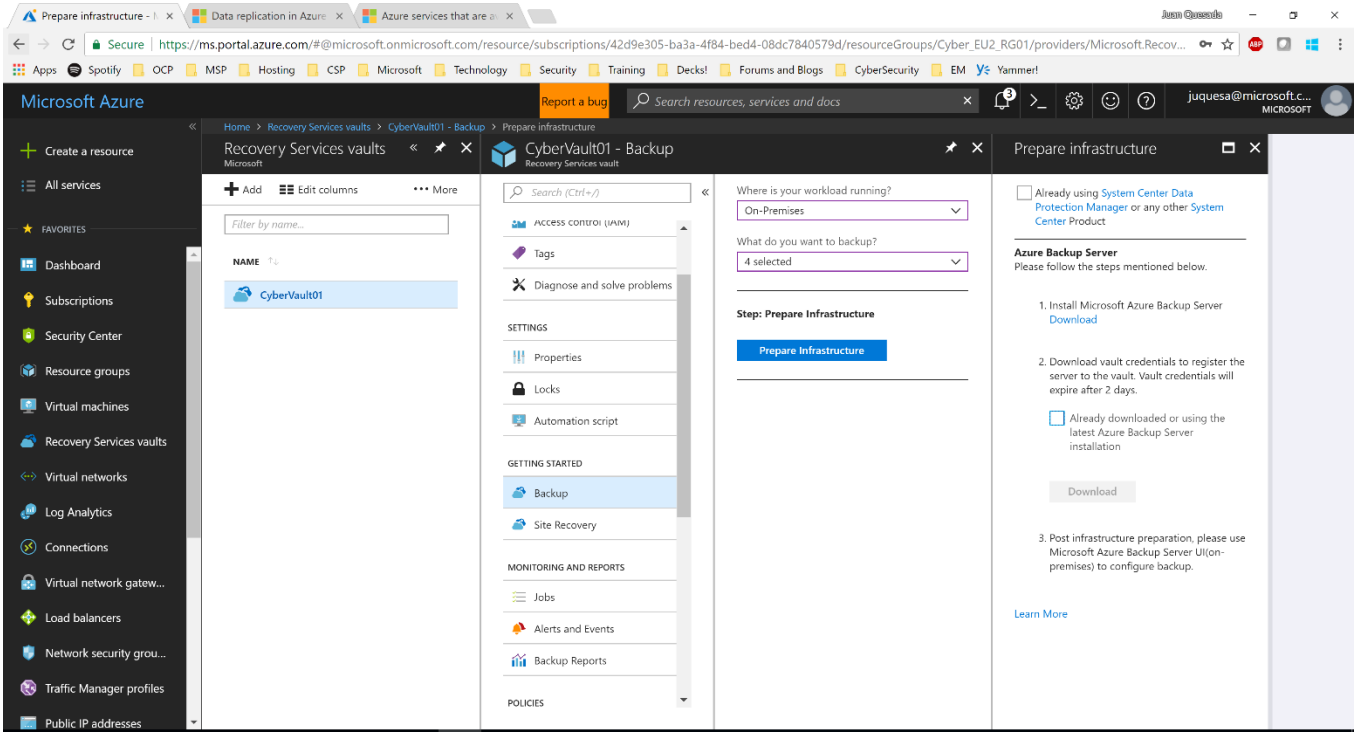
Para efectos de la guía, utilizaremos locally-redundant.



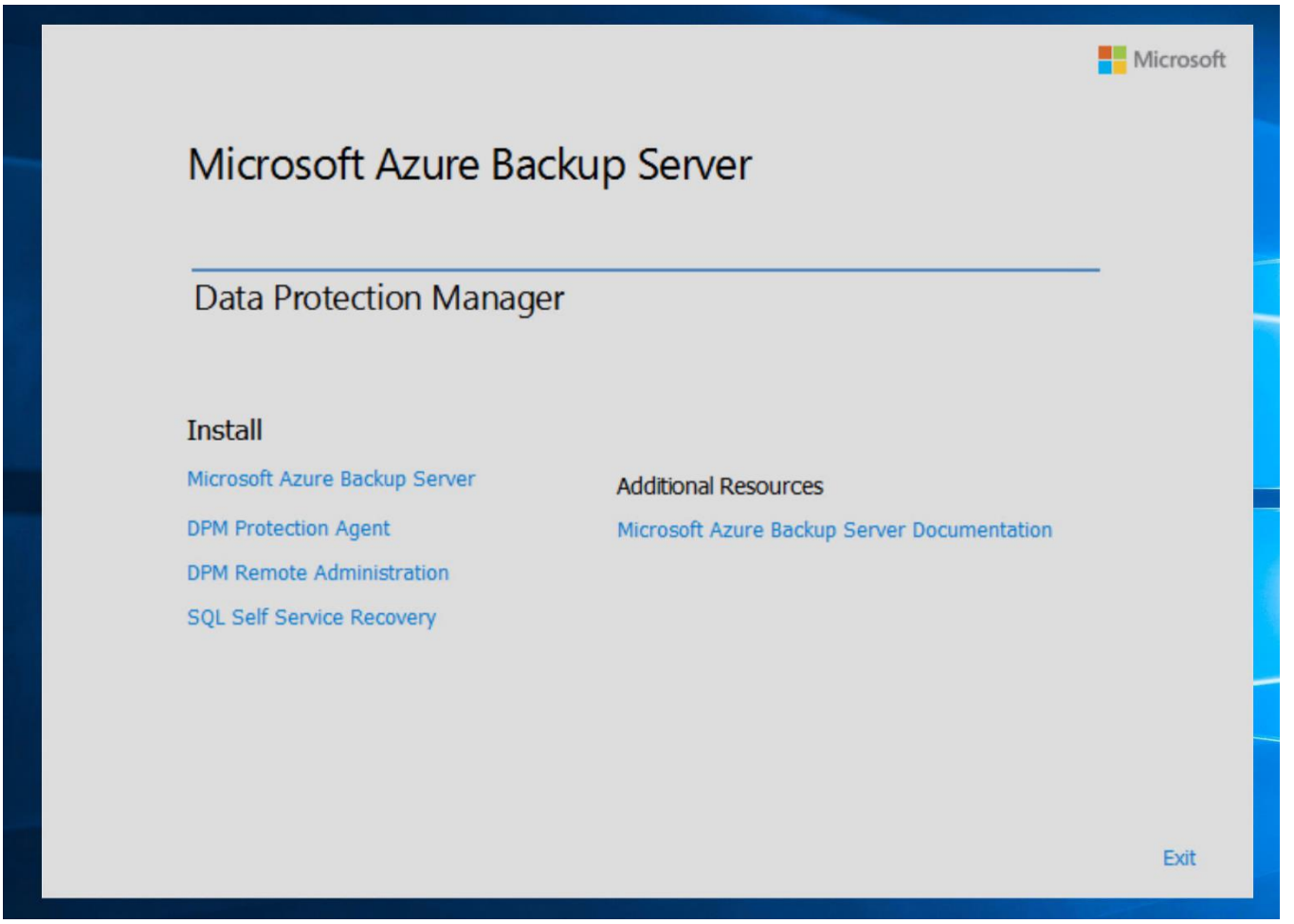
Luego en getting started, Backup, escogemos qué tipo de data queremos respaldar, solo archivos, SQL Server, Hyper-V/VMWare, entre otros.



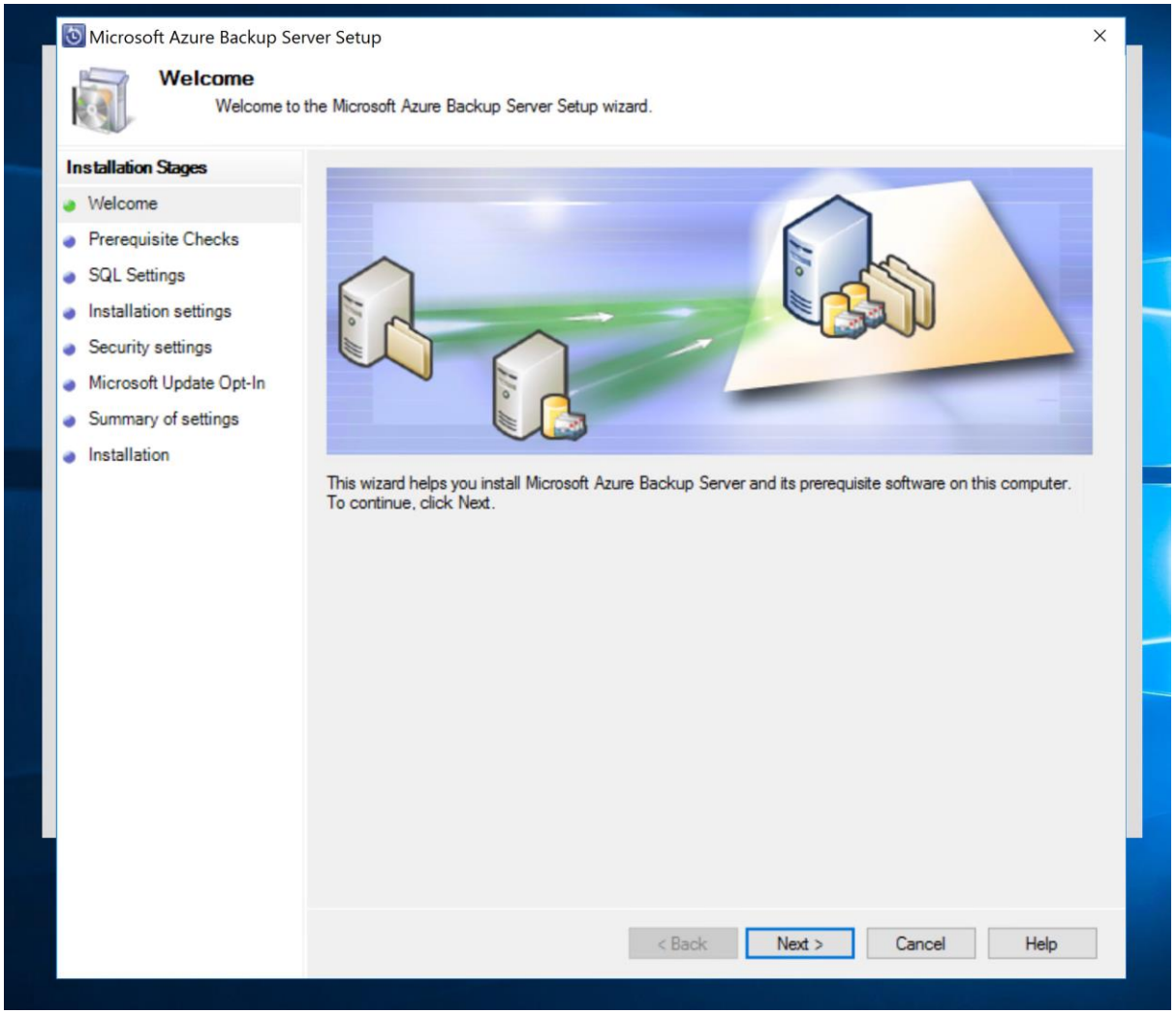
Esto nos habilita la opción de descargar tanto el instalador del Azure backup server, así como las credenciales de conexión. Procedemos a descargar ambas en el servidor designado para respaldos.



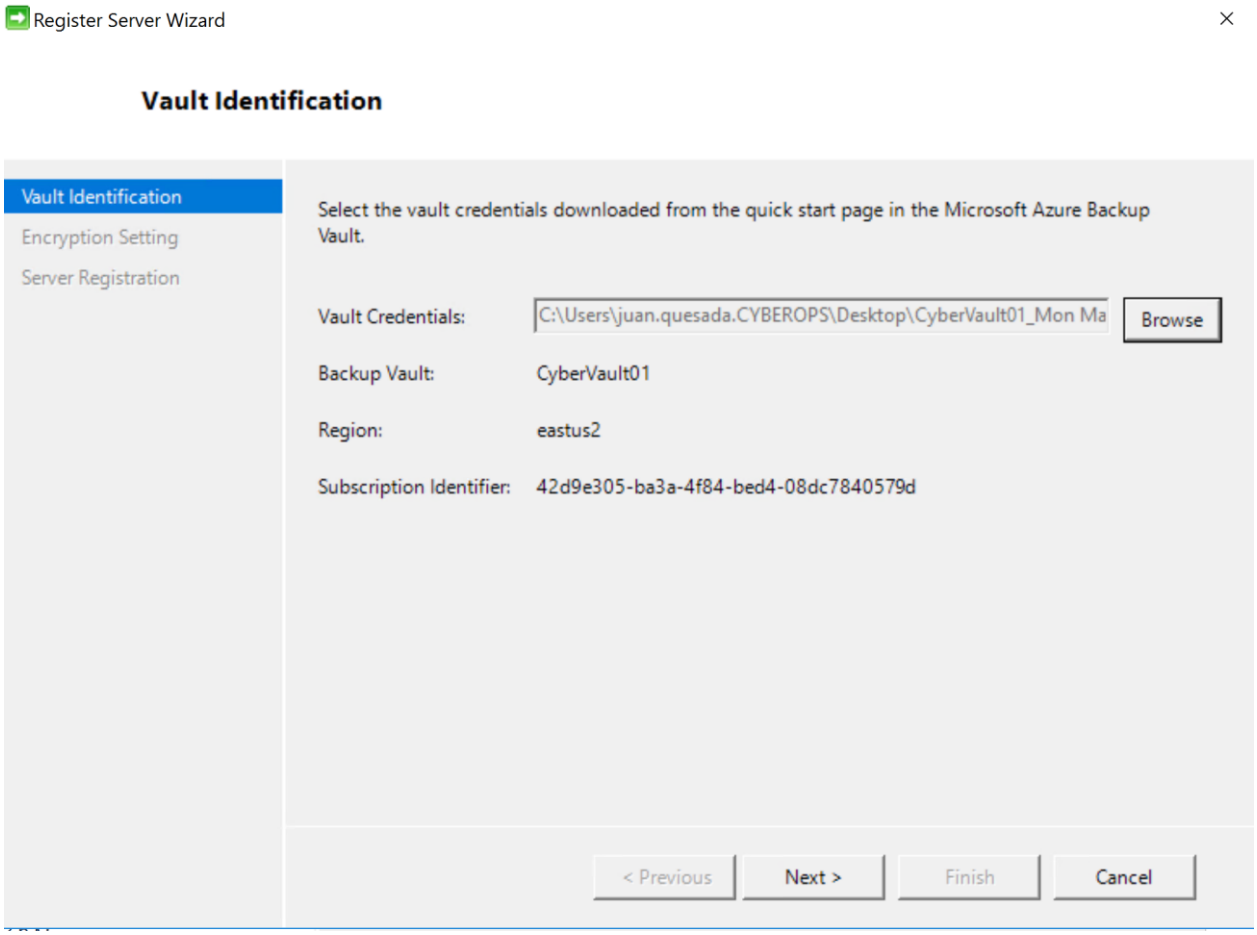
Ya por descargados los archivos, los descomprimimos y ejecutamos el instalador, lo cual nos abre la consola de instalación.



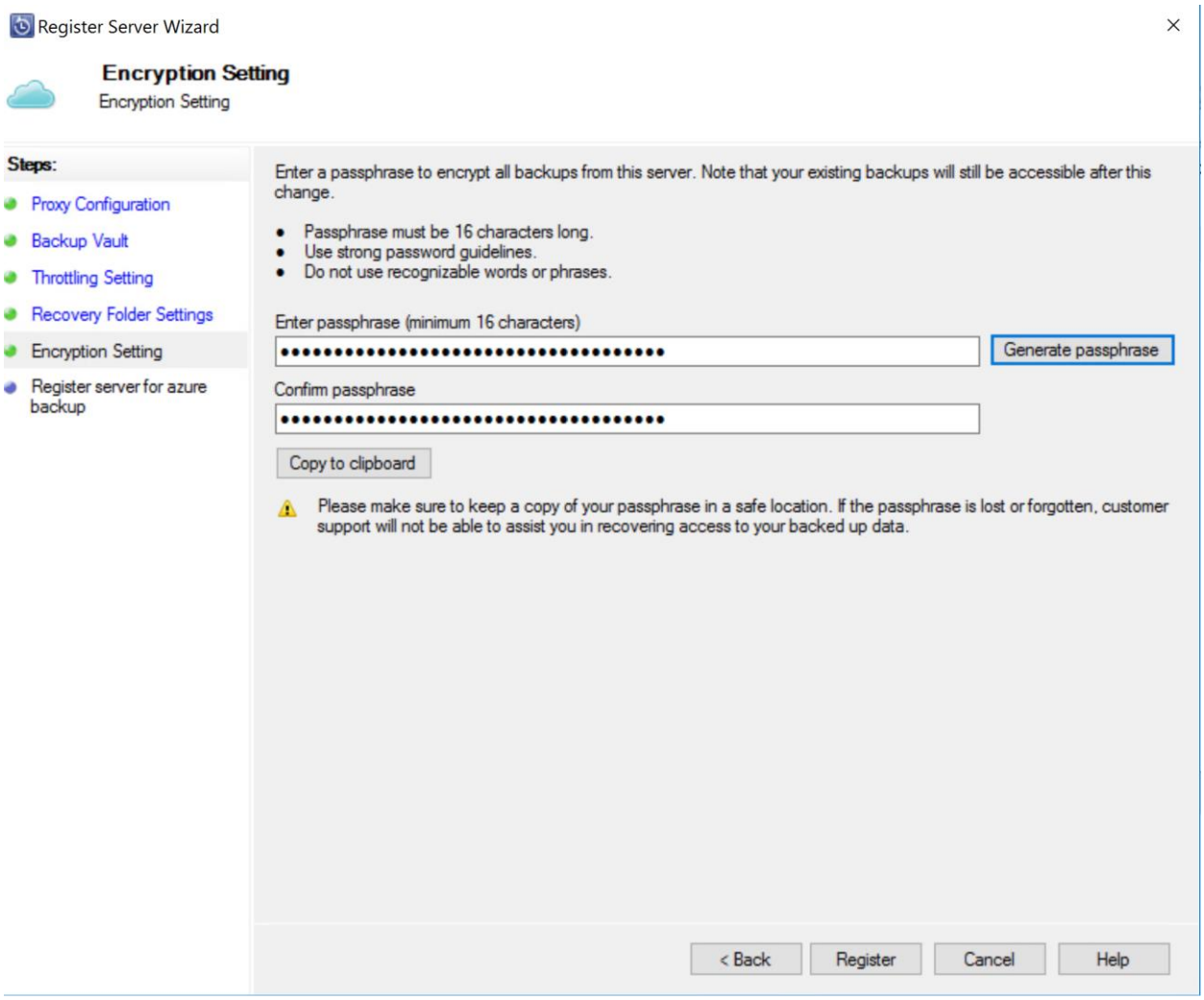
De aquí iniciamos el Microsoft Azure backup Server install.



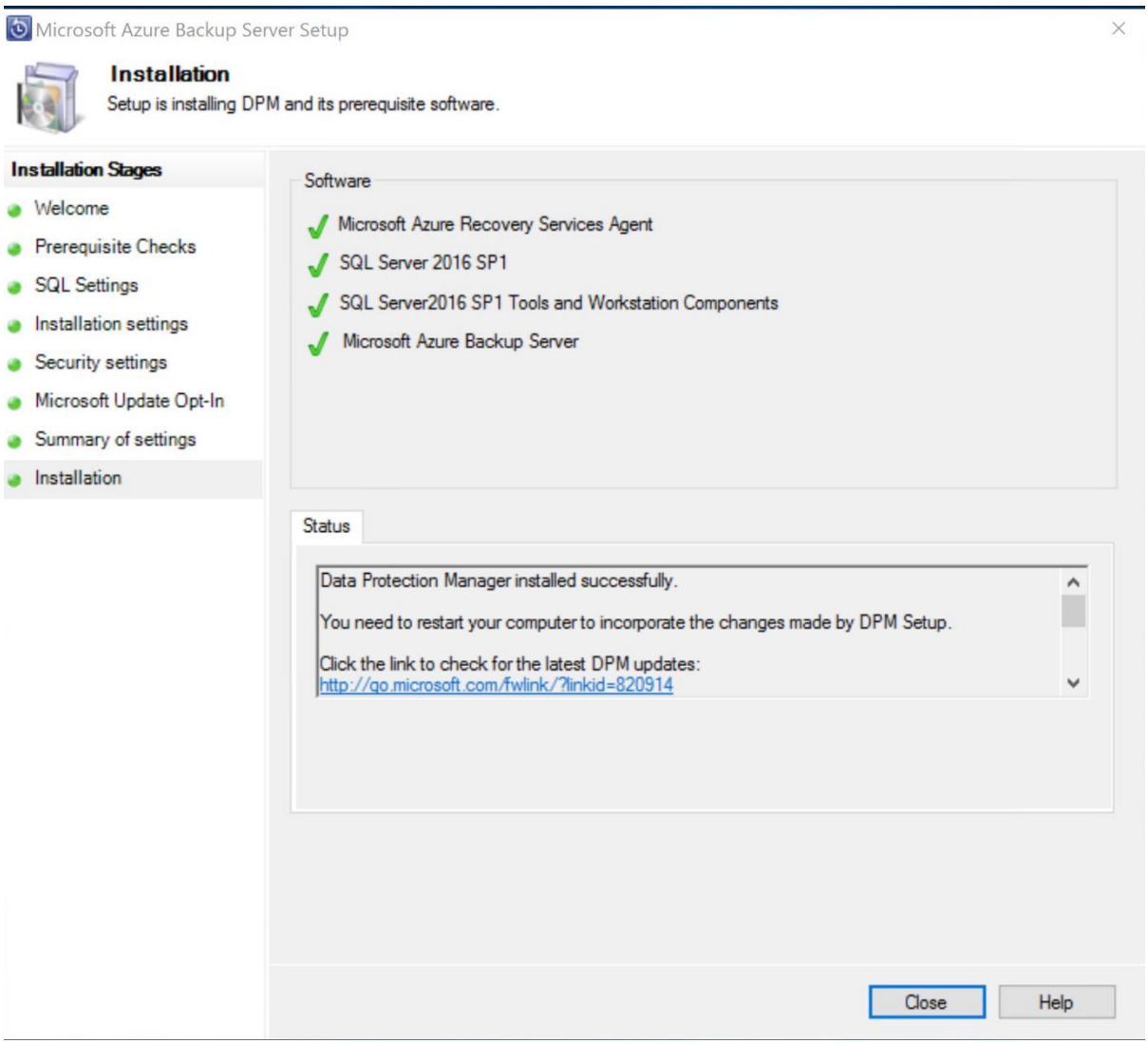
Es importante cumplir con todos los prerrequisitos que el instalador nos indica, como módulos y base de datos, para que el resultado final sea una implementación exitosa. Es fundamental importar las credenciales que descargamos anteriormente.



Durante la instalación, el sistema nos pide una frase de encripción, esta frase la debemos guardar ya que los respaldos están encriptados y sin esta no podremos acceder a la información. Es importante que se tenga una copia de esta frase fuera del servidor y resguardada por personal autorizado para tener dicha información, como una jefatura o gerencia.

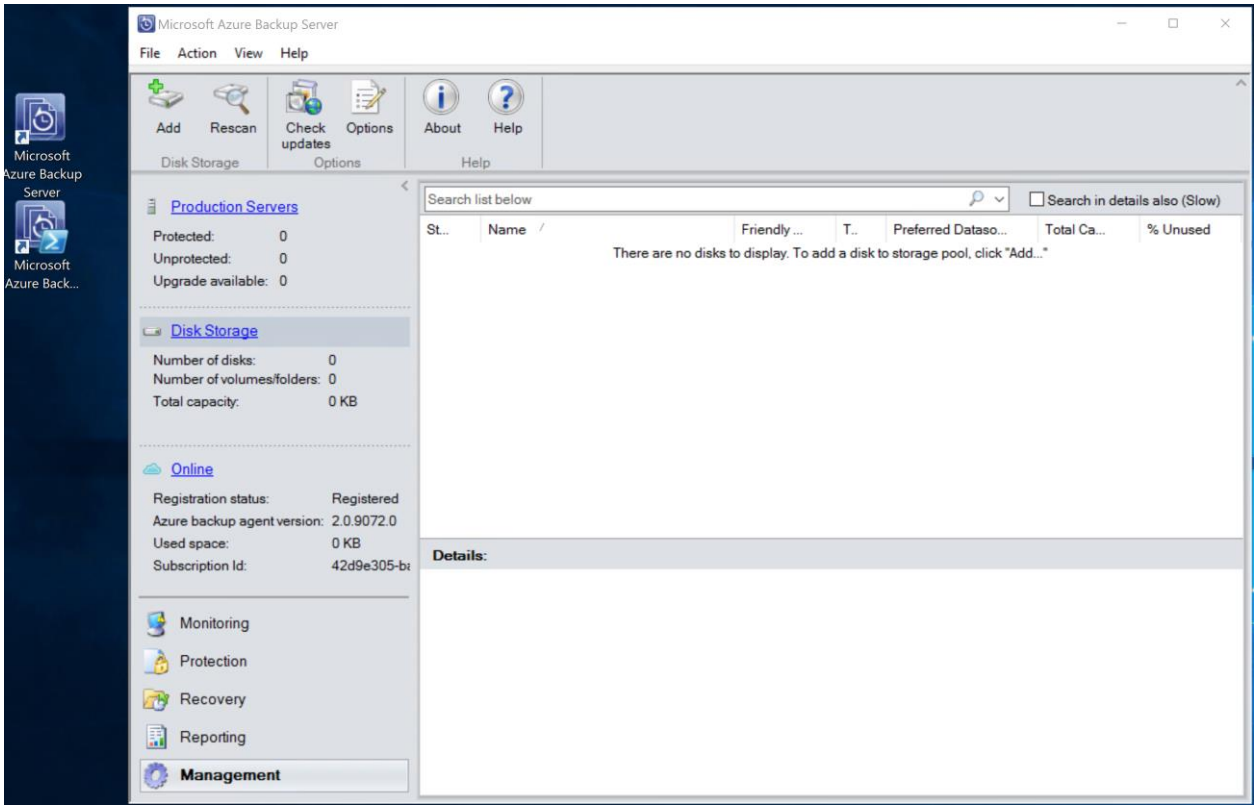


Por último, verificamos la instalación completa y corregimos si existe algún error.

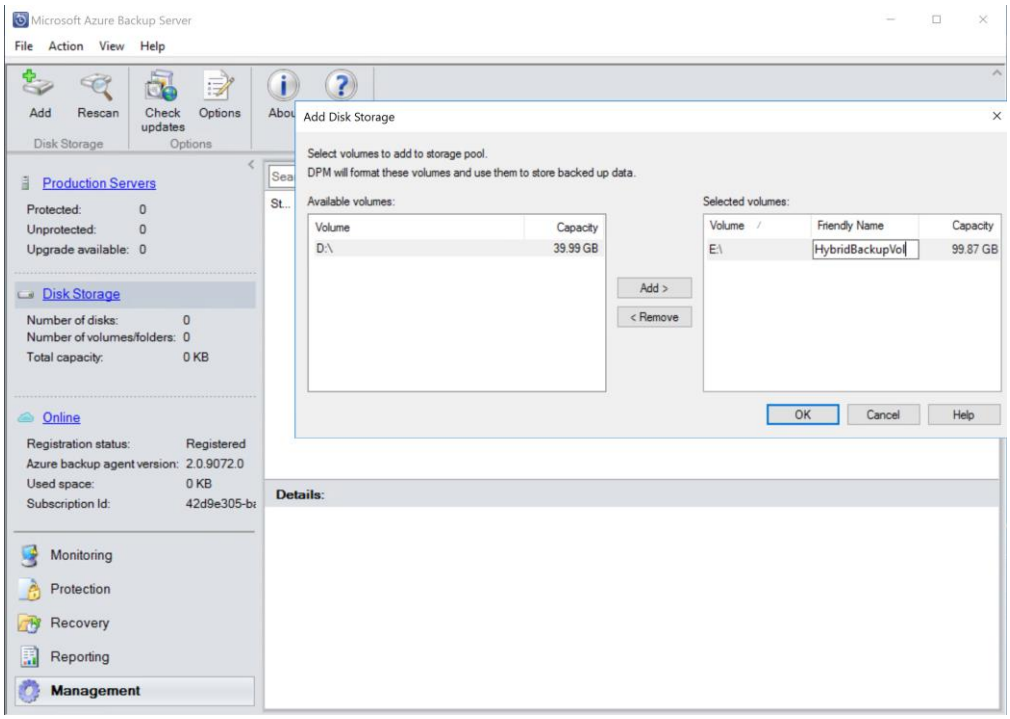


Configuración inicial del Backup Server

Entramos a la consola del Azure Backup Server, ícono normalmente en el escritorio o bien en programas, y navegamos a Microsoft Azure Backup Server.

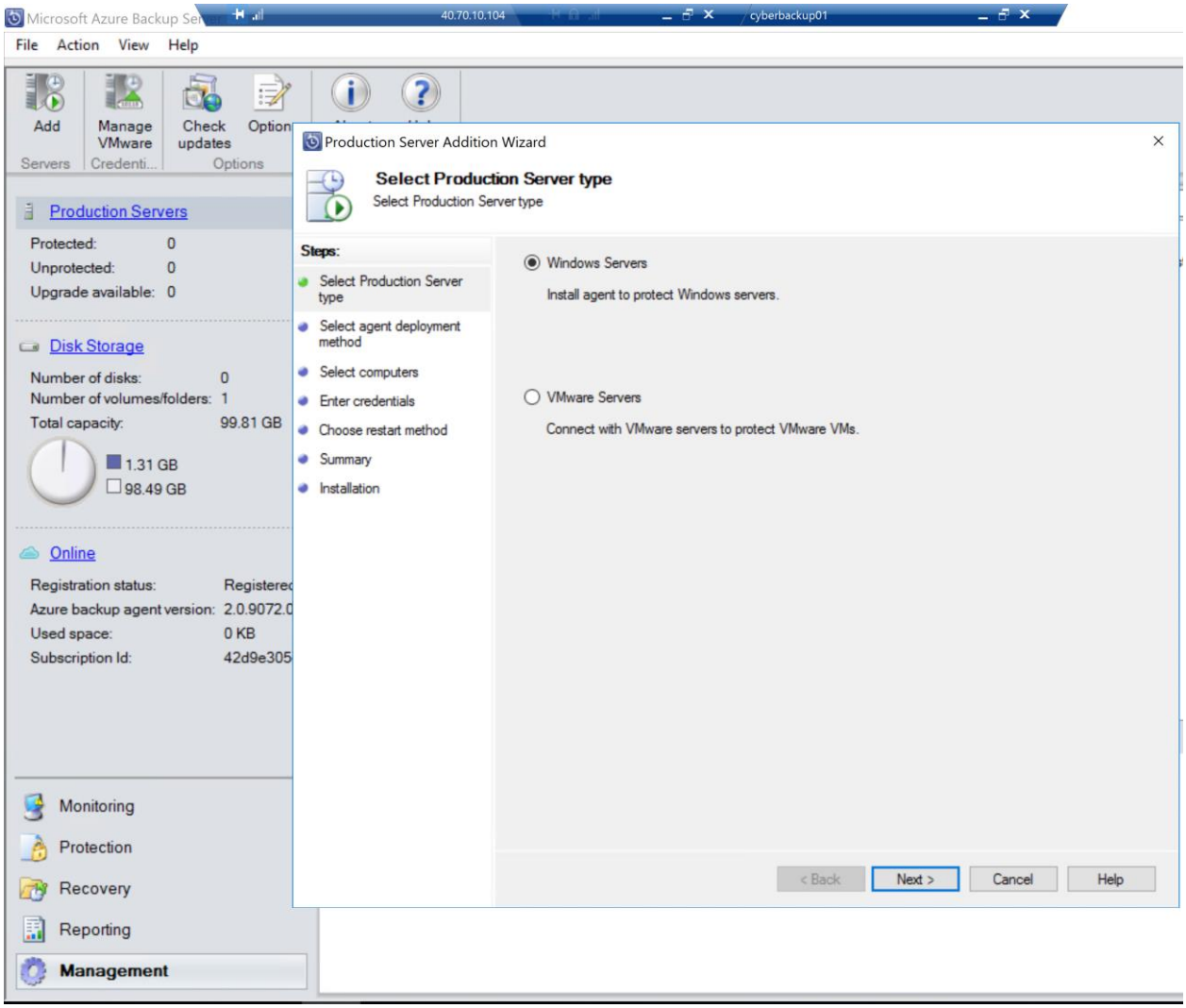


Lo primero que debemos hacer es agregar el espacio en disco que definimos para la copia local de datos, en Management damos clic en disk storage y add.

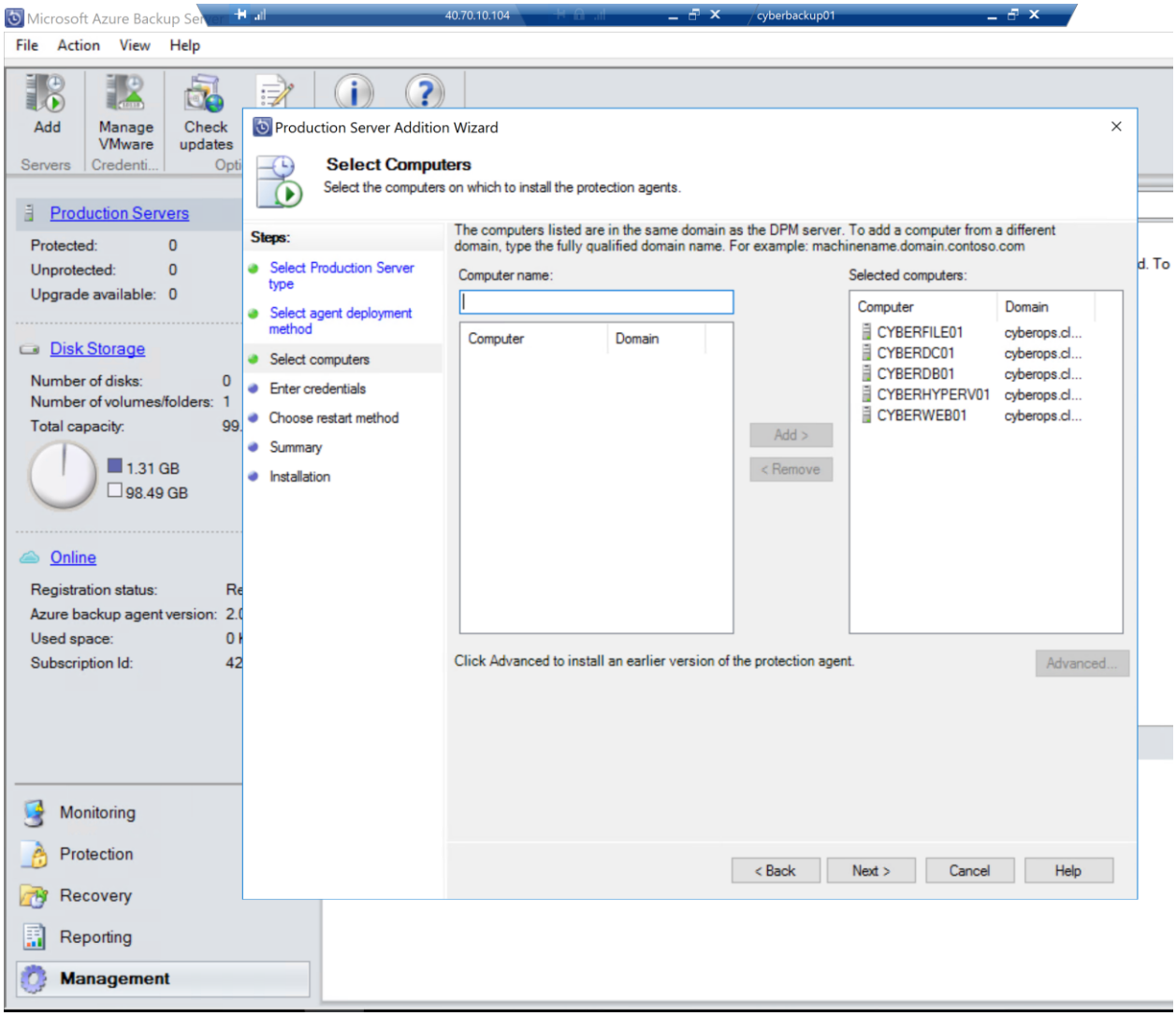


Luego, agregamos los servidores del dominio que requieren backup. Para efectos de nuestro ambiente tenemos varios servidores de diferentes funciones, aunque pueden variar en su realidad, los mismos son comunes un ambiente pymes.

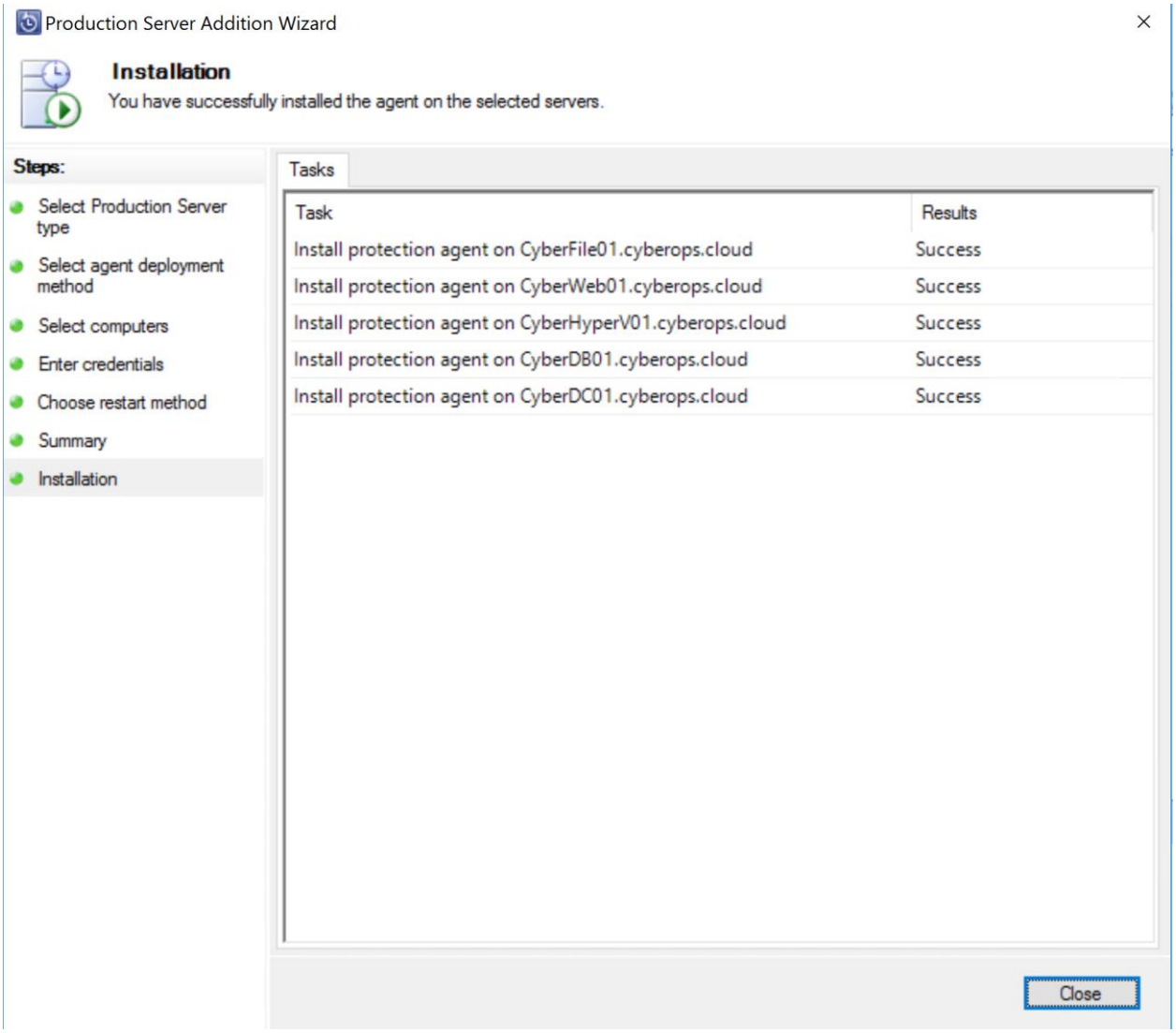
- Controlador de Dominio (dominio, identidad usuarios y políticas).
- Servidor de SQL Server (base datos de la empresa).
- Servidor Web (ya sea intranet o página web comercial a clientes).
- Servidor de Archivos (repositorio de archivos y documentos de la empresa).
- Servidor Hyper-V (servidor de virtualización de máquinas virtuales).



Seleccionamos los servidores a instalar el agente.



Por último, verificamos la instalación correcta.



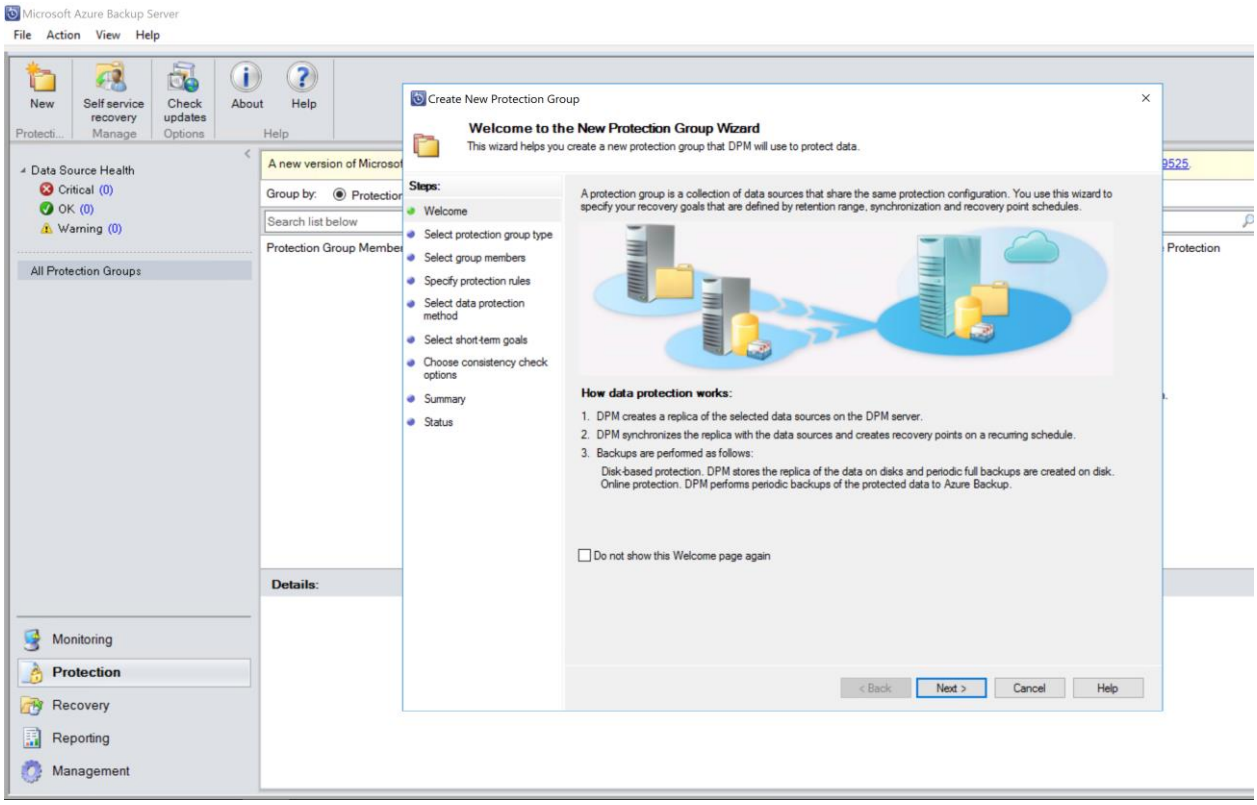
Configuración de respaldos

Los respaldos se configuran de varias maneras, ejemplos:

- Comparten la misma política de respaldo, por ejemplo, respaldos diarios a la misma hora.
- Comparten el mismo servicio, por ejemplo, todos son servidores web.
- Individual o grupos pequeños.

Para esta guía, vamos a configurar todos los servidores de manera individual para resaltar los detalles de la configuración de cada uno.

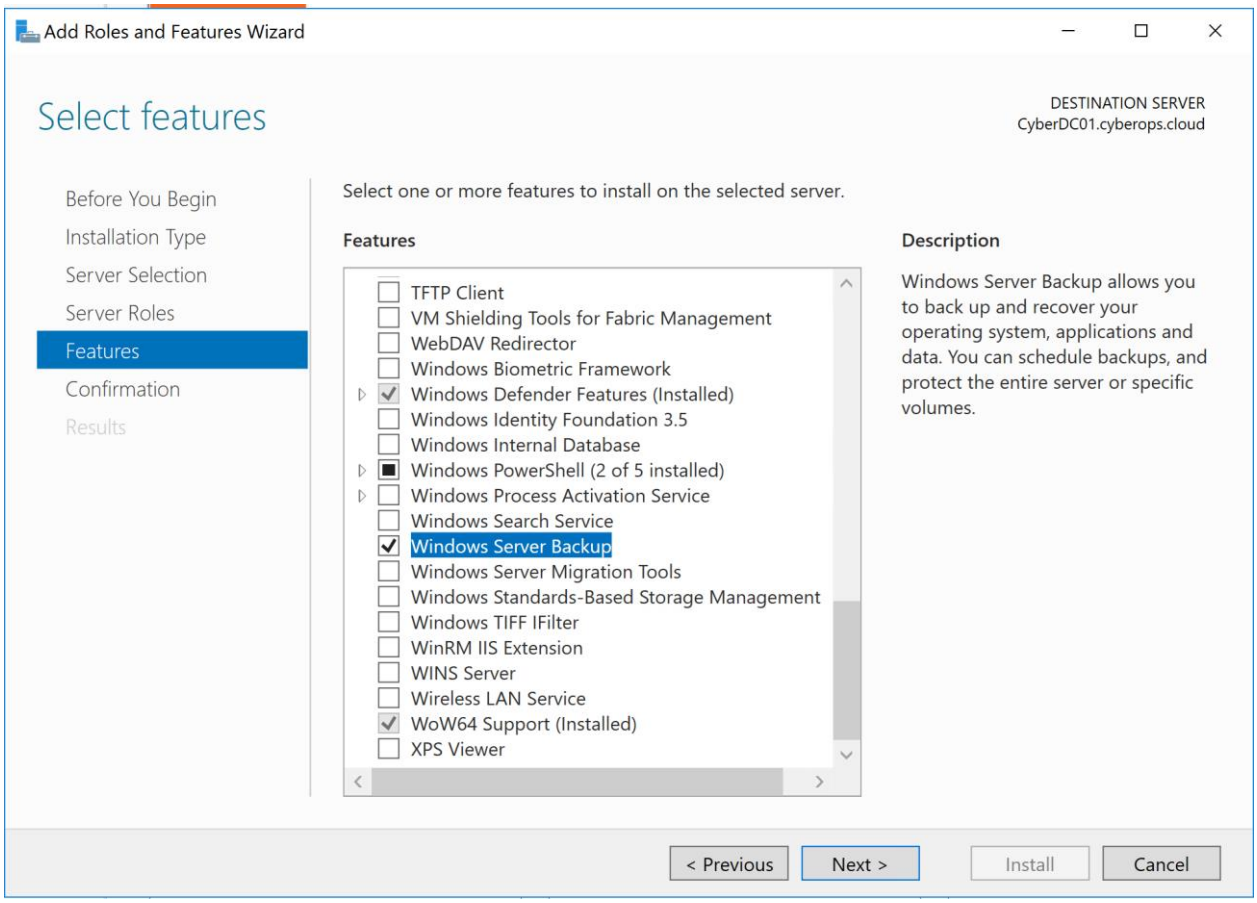
De manera genérica, la configuración de respaldos de todos los servidores inicia de la misma manera y esto es en protección, agregar nuevo grupo de protección y configurar los específicos del respaldo.



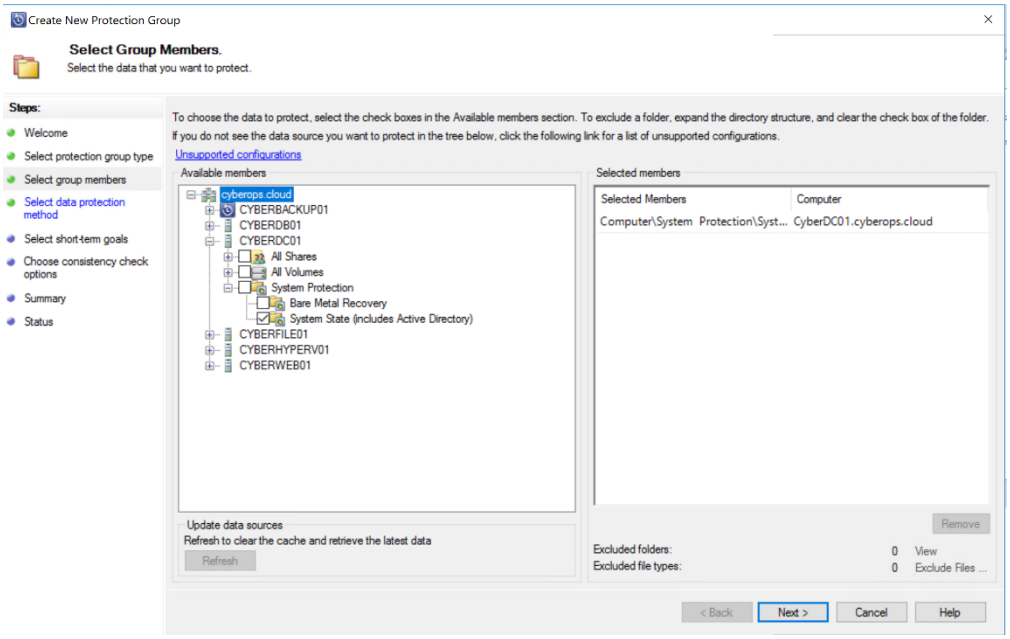
Controlador de Dominio

Como prerrequisitos: Es importante que el usuario que ejecute la tarea de respaldo sobre un controlador de dominio tenga los suficientes privilegios de respaldo, para este ejercicio el administrador de dominio es quien ejecutará la tarea.

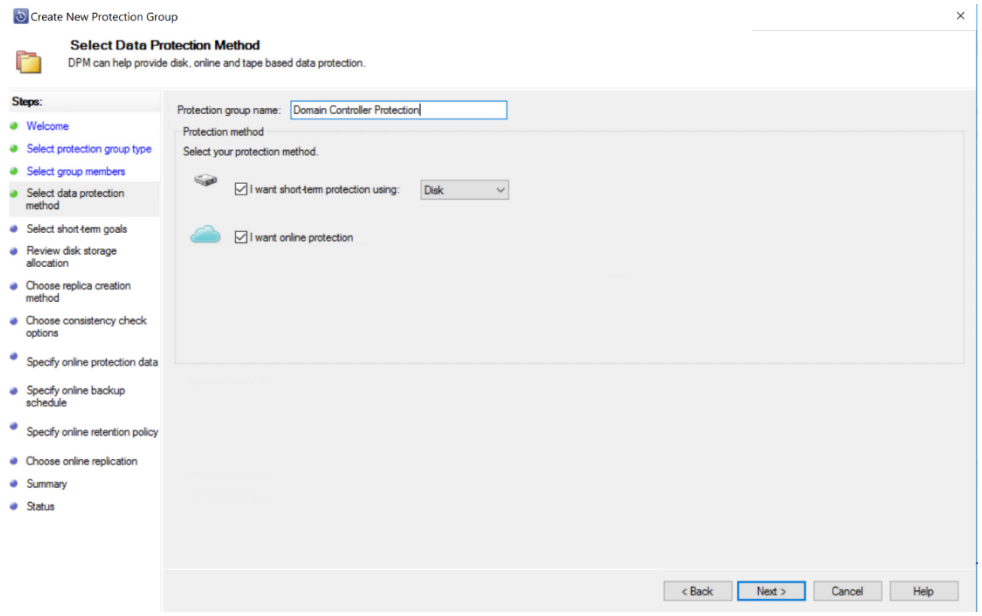
Se debe instalar el Windows Server Backup feature local al servidor, esto desde el administrador de tareas.



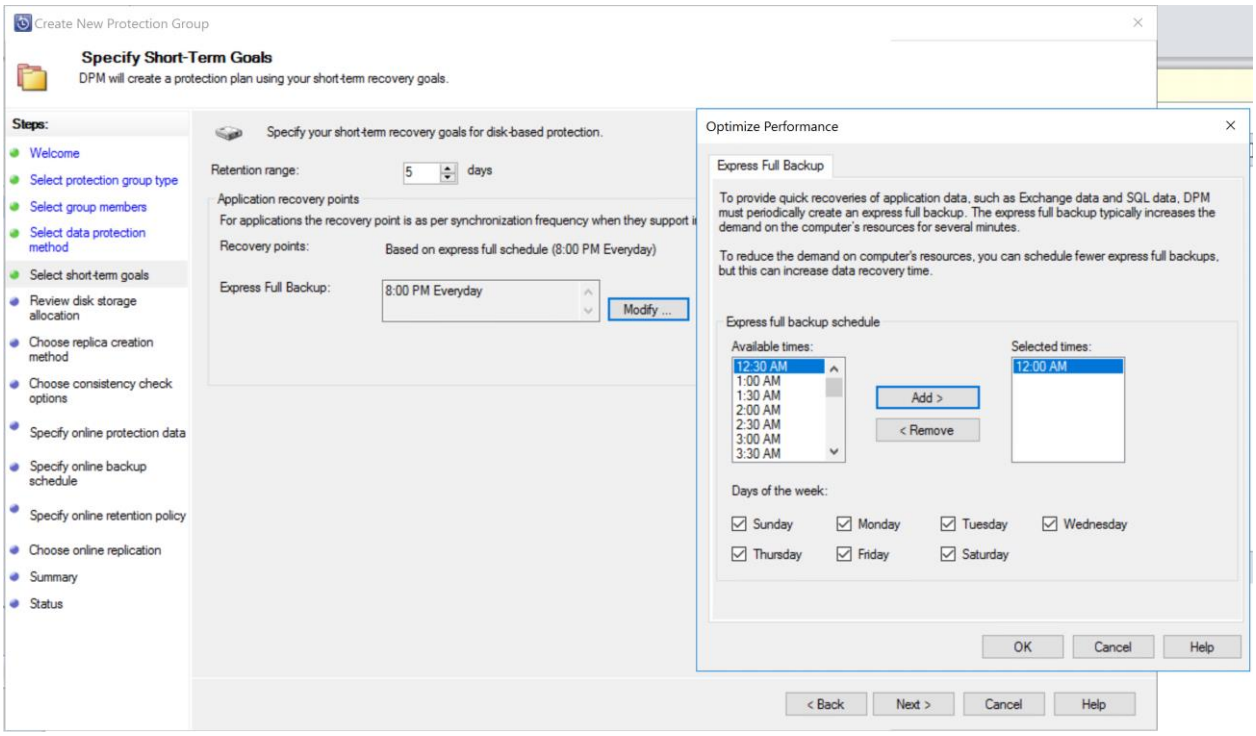
Seleccionamos el servidor, expandimos las opciones y seleccionamos System State (Includes Active Directory).



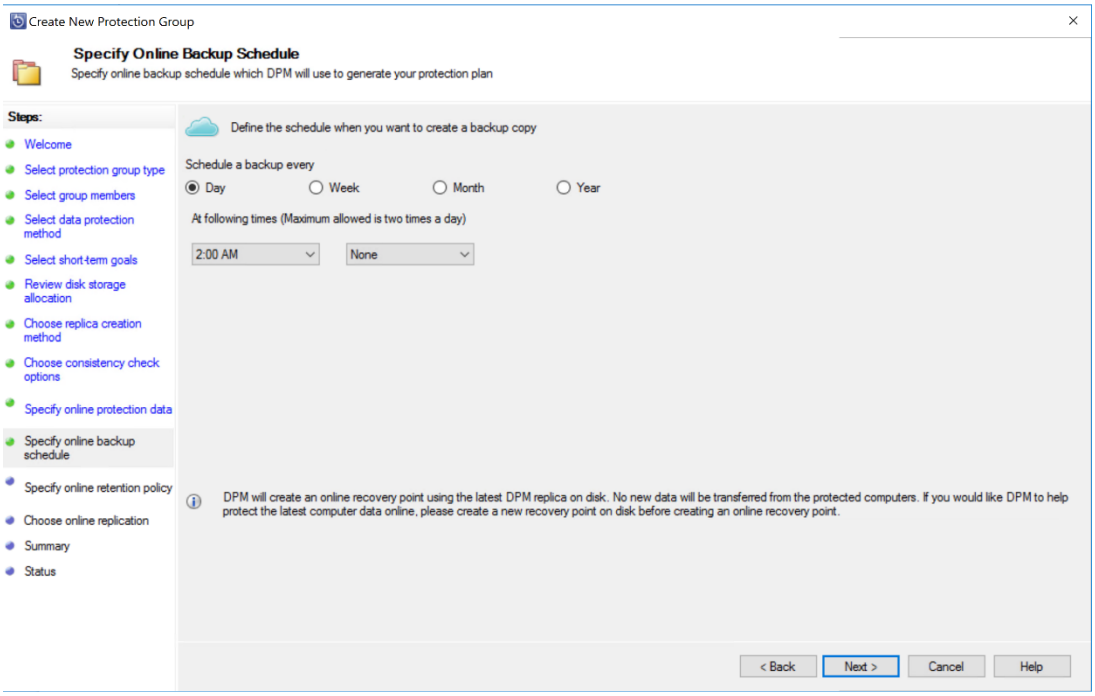
Le damos un nombre y seleccionamos respaldo a disco y en la nube.



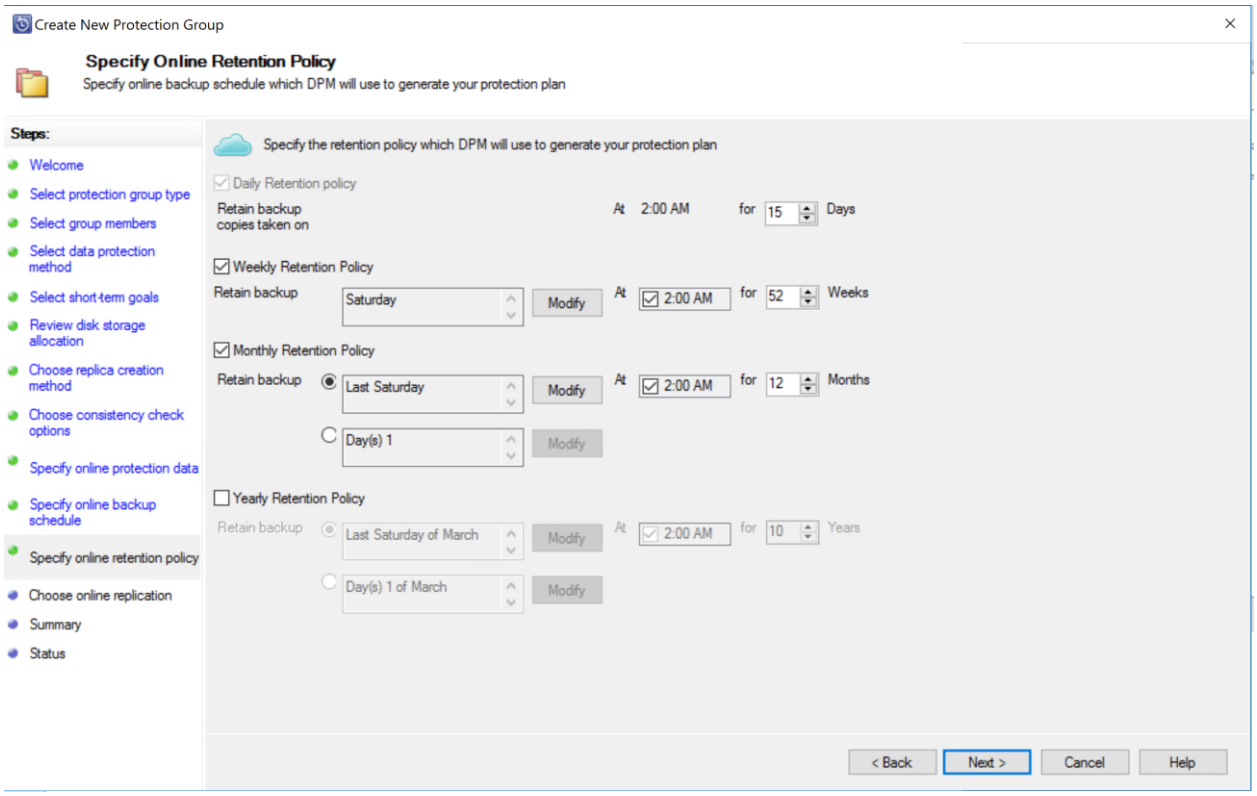
Especificamos la retención de disco, la cual se refiere a cuánto tiempo los datos respaldados se mantendrán asegurados. Los mismos al momento de expirar serán eliminados automáticamente, esto nos asegura que la data del respaldo se mantendrá por un mínimo de días y a la vez asegura que estamos liberando espacio para los siguientes respaldos. Además, podemos configurar la periodicidad de los respaldos, entre las opciones qué días y qué horas, incluso múltiples veces por día.



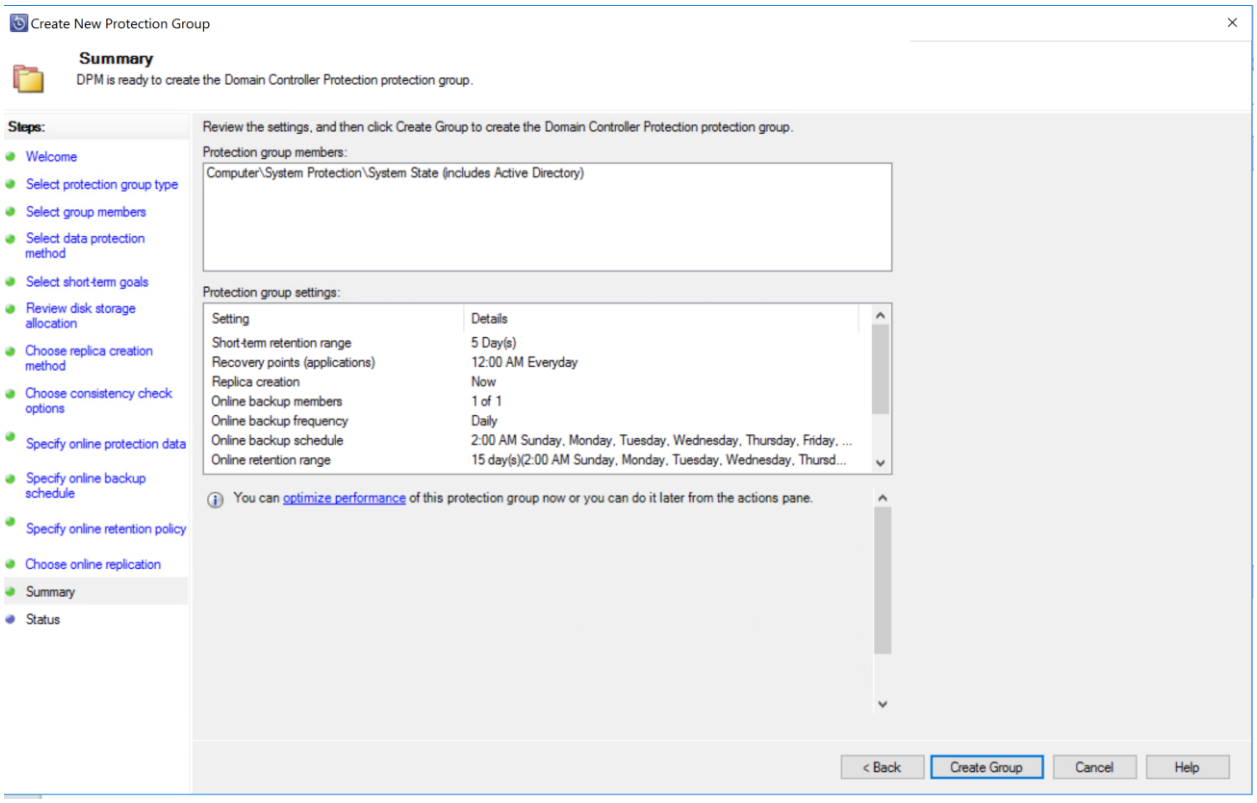
Luego escogemos cuándo queremos que los respaldos se sincronicen hacia la nube, recordemos que estos respaldos van a través del enlace de internet, por lo que se recomienda sea fuera de horario laboral y posterior a que el respaldo se haga en disco. Aunque el respaldo a disco sea diario, podemos escoger que los datos respaldados a la nube tengan diferente esquema de sincronización.



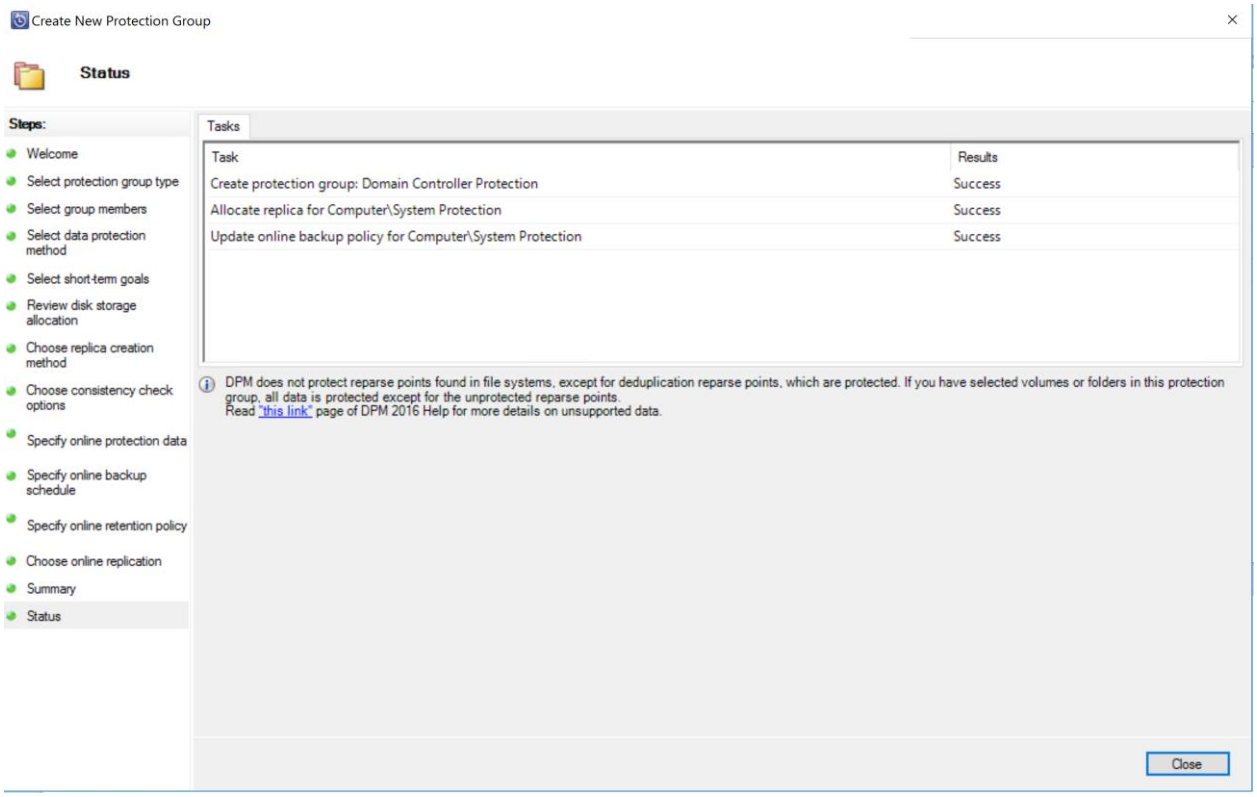
Seguidamente, escogemos la retención de los datos en la nube, lo cual funciona igual al de disco recientemente mencionado. Aquí la diferencia es que queremos un respaldo a disco por pocos días para no consumir mucho espacio de disco local y también para poder restaurar de manera rápida, dado que la velocidad de un disco local es mucho más rápida a un enlace de internet en la nube. Es importante recalcar que el disco local y la nube, al ser dos ubicaciones distintas, es un respaldo que se considera apto para recuperarse en un desastre, es decir cuando el sitio local sufre algún daño irreversible.



Como penúltimo paso, verificamos la configuración correcta, nos devolvemos a reconfigurar si es necesario algún cambio.

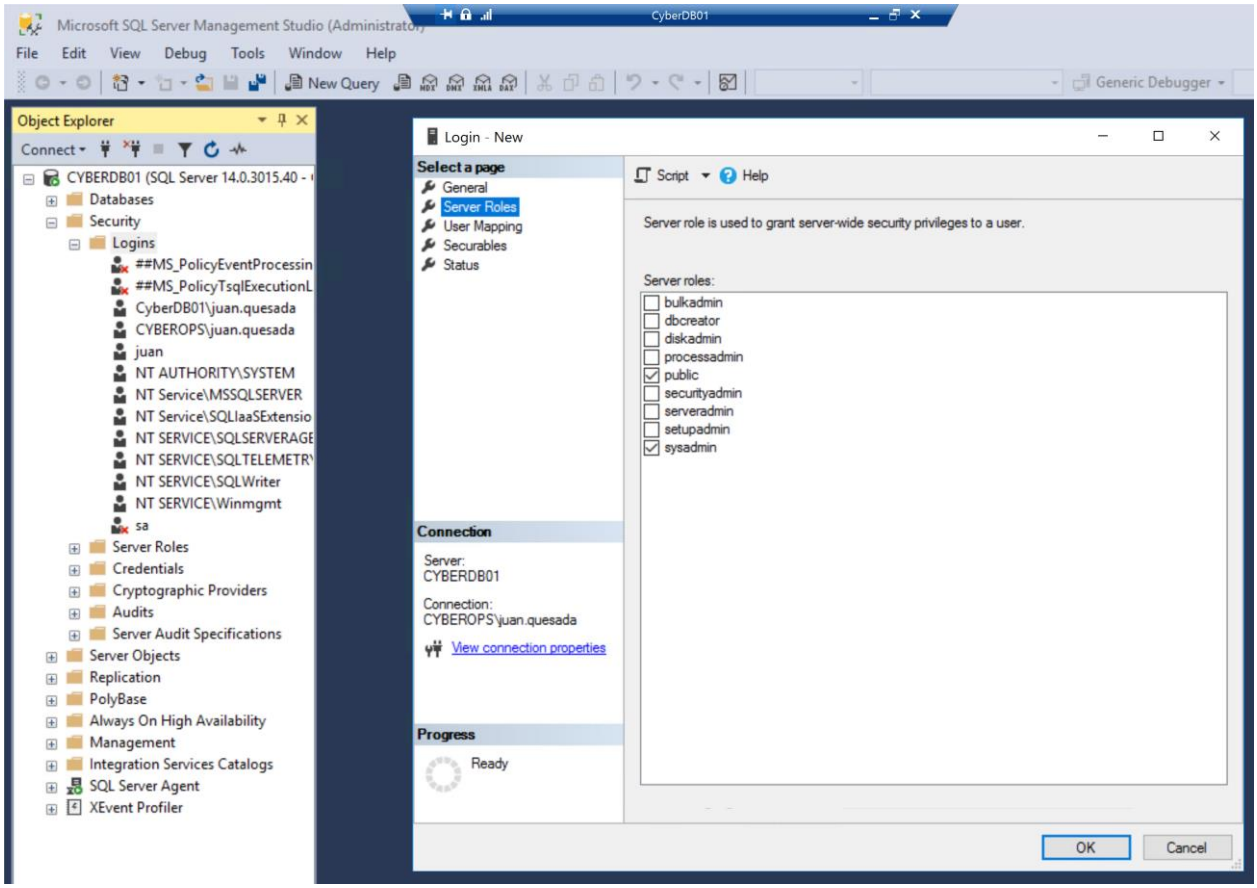


Para cerrar, verificamos que el respaldo se configure y ejecute correctamente.

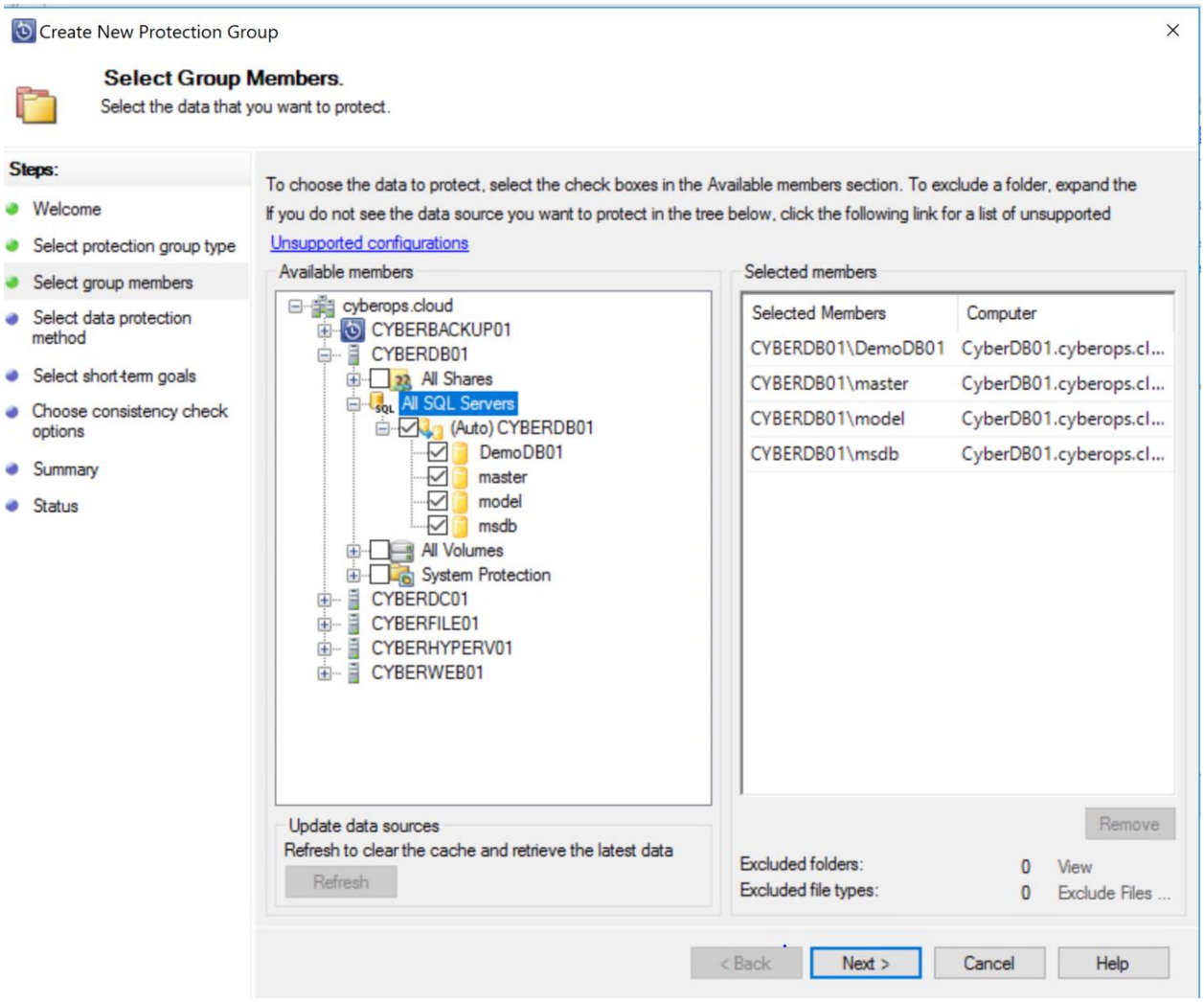


Servidor de Base de Datos

Como prerrequisito de backup, debemos agregar al usuario NT SERVICE\DPMRA como sysadmin de la base de datos. Para esto ingresamos al servidor y desde el SQL Management Studio, en logins, agregamos manualmente al usuario con privilegios sysadmin.

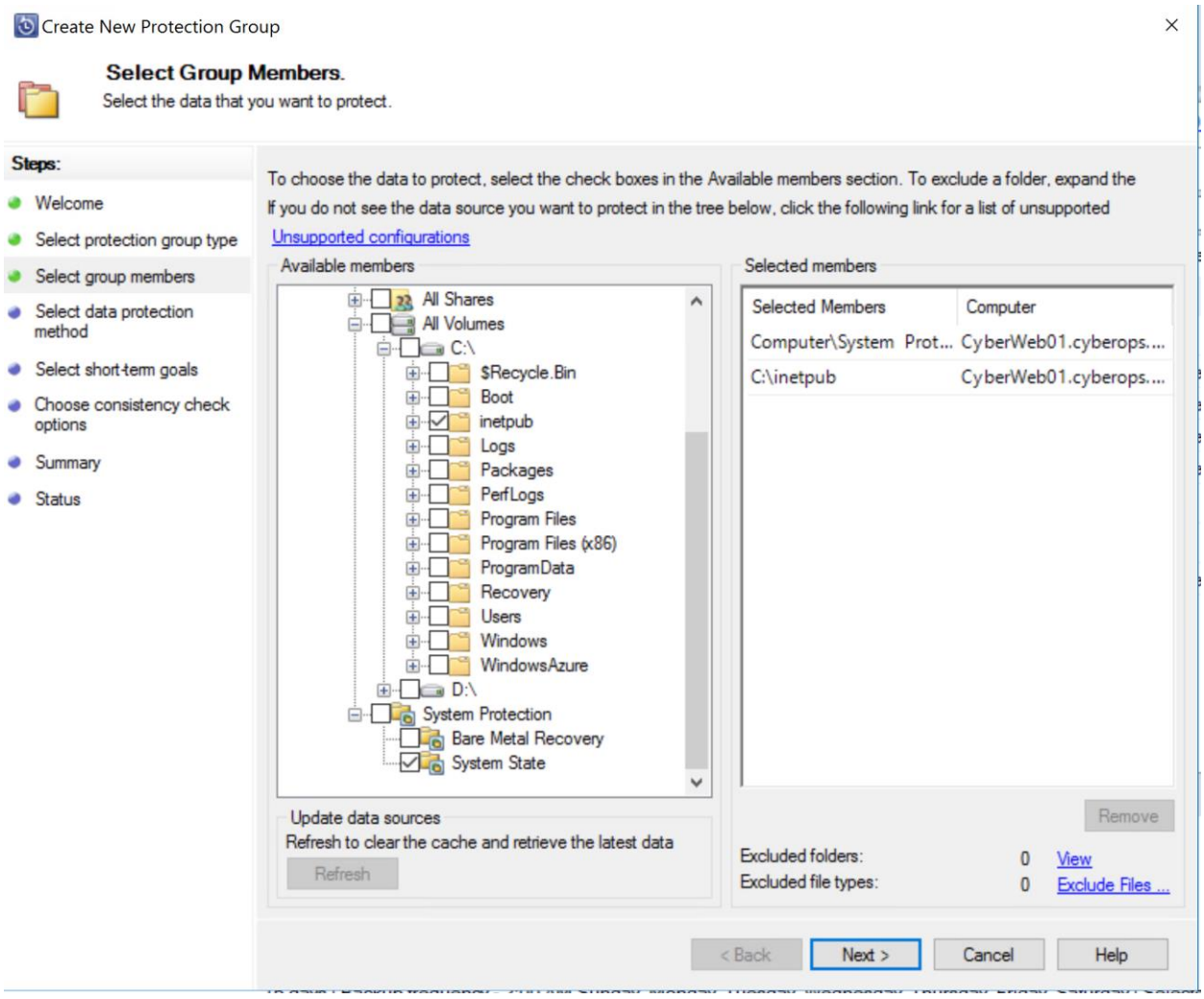


Seguimos los mismos pasos iniciales del respaldo al controlador de dominio, con la diferencia de que aquí escogemos las bases de datos y cambiamos las políticas de respaldos y retención según la necesidad propia de la empresa. Normalmente las bases de datos se respaldan varias veces por día para asegurar tener respaldada la máxima cantidad de datos en caso de una eventualidad.



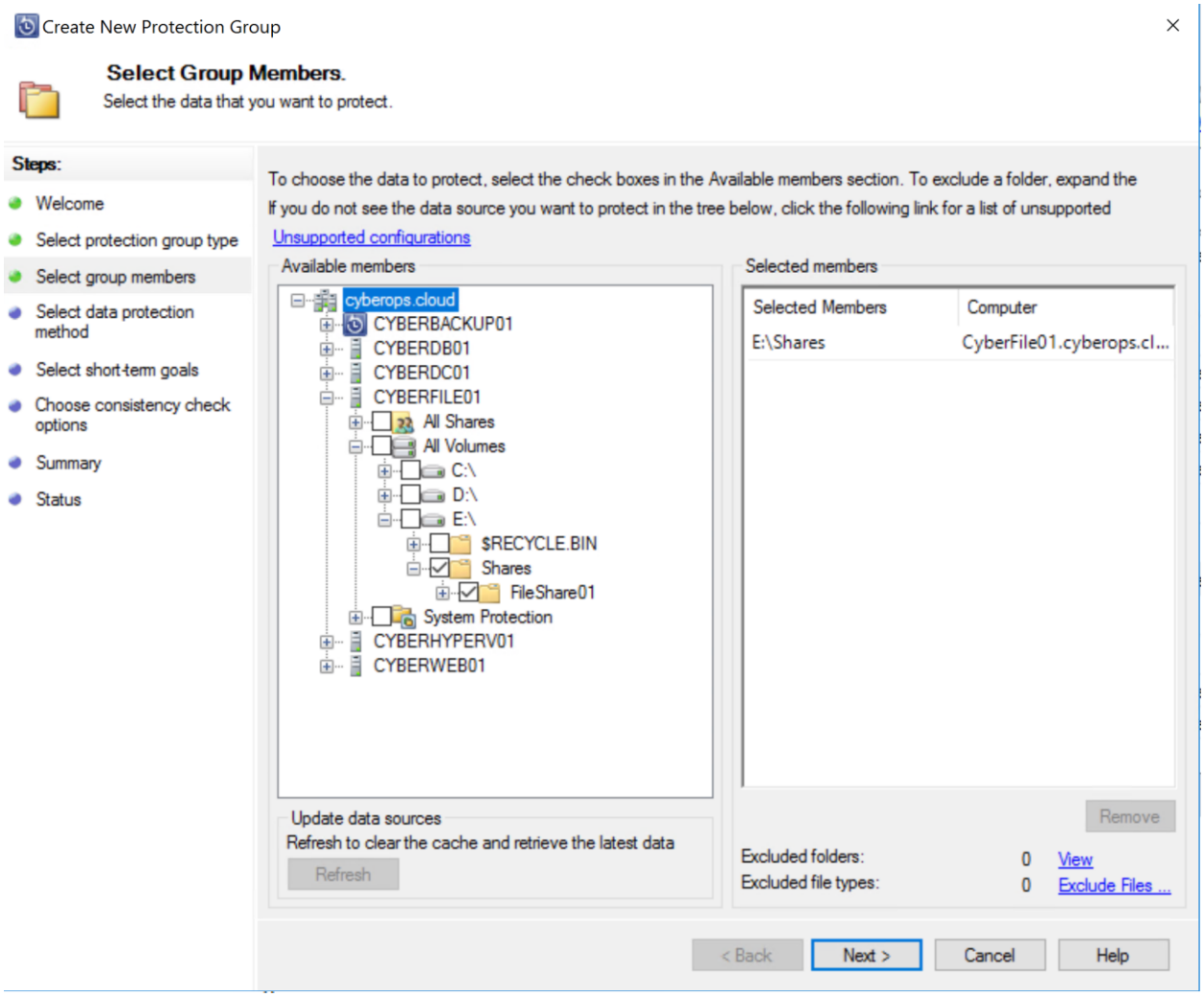
Servidor Web

Como prerrequisito, debemos instalar el Windows server backup feature mostrado anteriormente en la configuración del controlador de dominio. Seguimos los mismos iniciales mencionados anteriormente, se asegura que respaldemos el folder inetpub y el System state, esto nos garantiza poder guardar la información del sitio web.



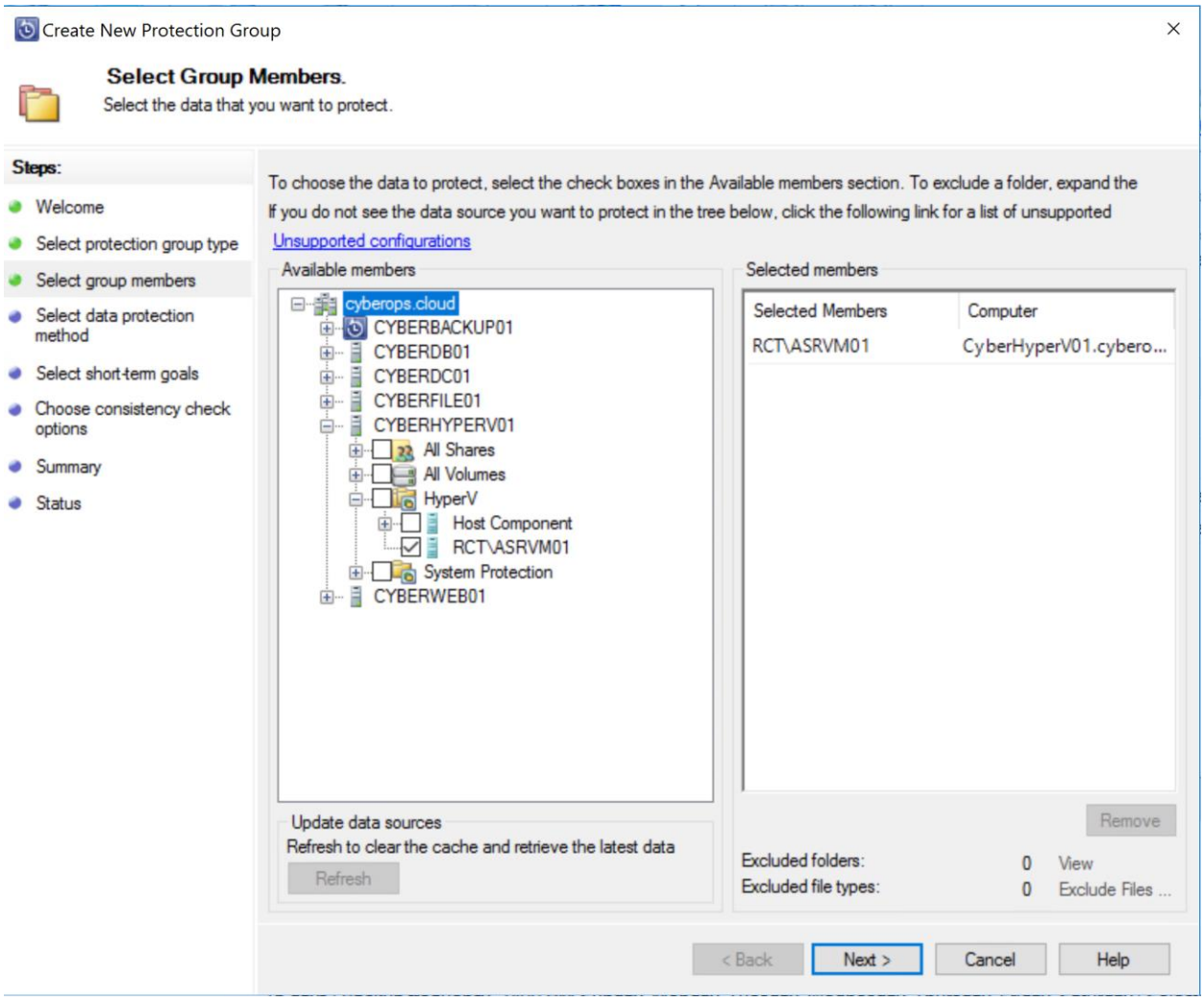
Servidor de archivos

Seguimos los mismos pasos iniciales anteriores, aquí la diferencia es que vamos a respaldar los volúmenes compartidos o shares.



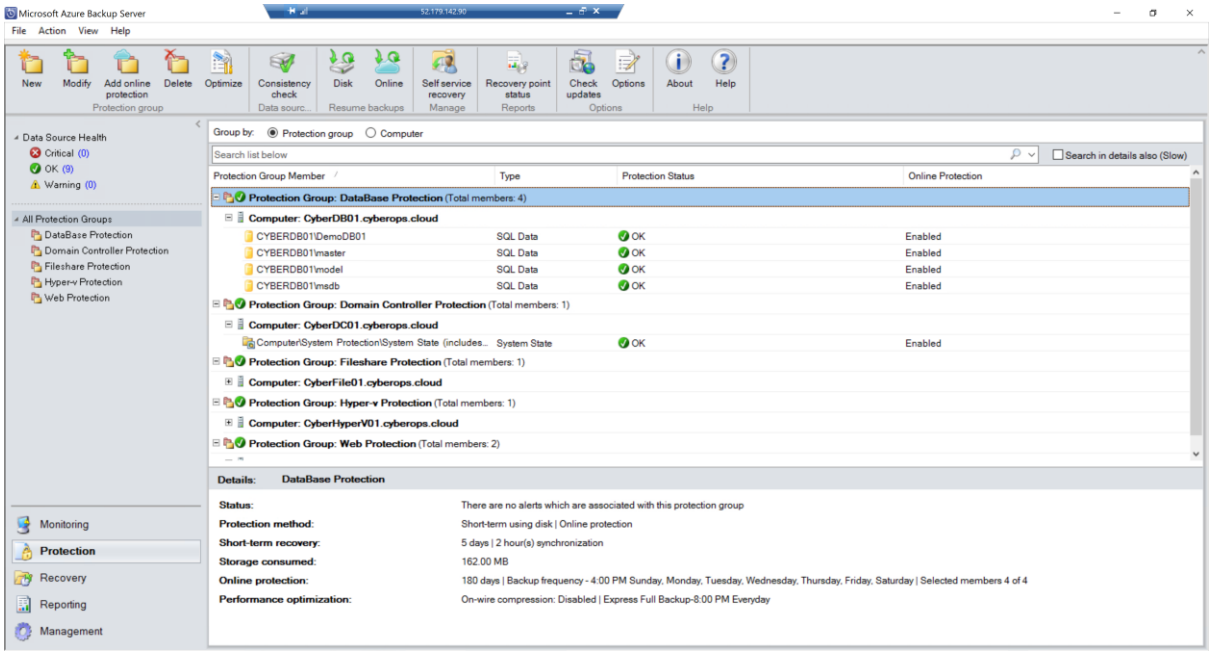
Servidor virtual

Seguimos los mismos pasos iniciales anteriores, acá la gran diferencia es que estaremos respaldando máquinas virtuales completas. De esta manera podremos con los respaldos anteriores recuperar la data o parte de ella de manera fácil y ágil, mientras que el respaldo a las máquinas virtuales nos permite recuperar el servidor con su configuración y data completa en un punto en el tiempo; este es un método muy efectivo para recuperarse de un servidor no funcional completo. Para efectos de la prueba tenemos un servidor llamado ASRVM01, el cual tiene Windows Server instalado. Otra variable es que no requerimos respaldar diariamente este servidor, sino que con una vez por semana suele ser suficiente.

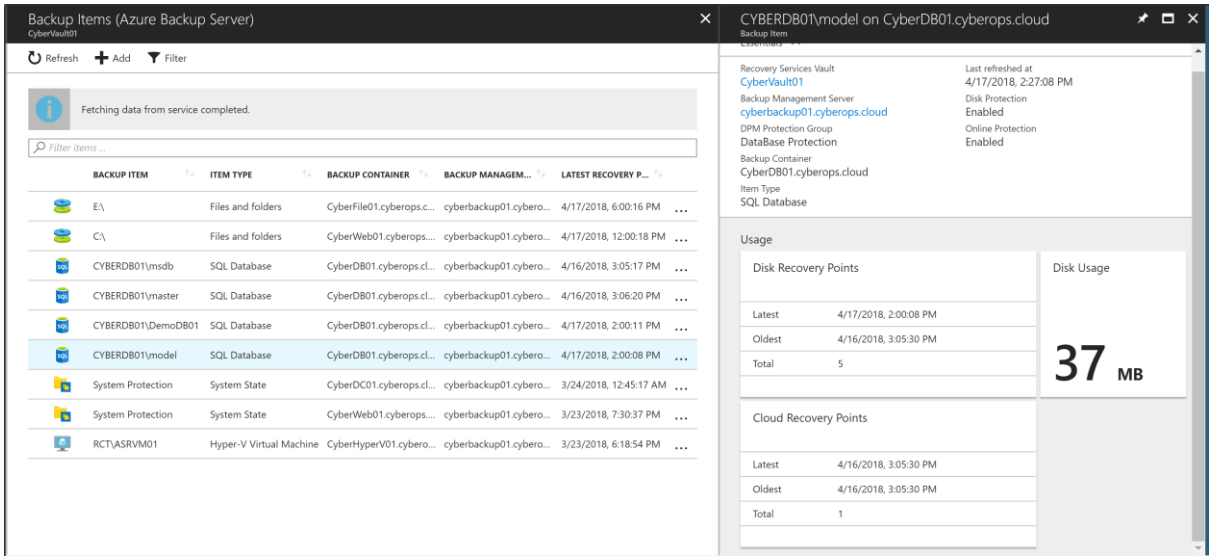


Verificación

Es importante, luego de la configuración de los respaldos, verificar que los mismos se estén ejecutando correctamente y que se estén sincronizando contra la bóveda en la nube. Desde el Azure Backup Server, en protección podemos fácilmente ver la salud de todos los respaldos.



De igual manera podemos mirar el estado de los respaldos en el portal de Azure, ya que el mismo se comunica con la herramienta de respaldo. Es importante validar que existan Cloud recovery points ya que son los que nos permiten recuperar datos desde la nube. Los mismos aparecerán posteriores a la fecha que indicamos durante la configuración.



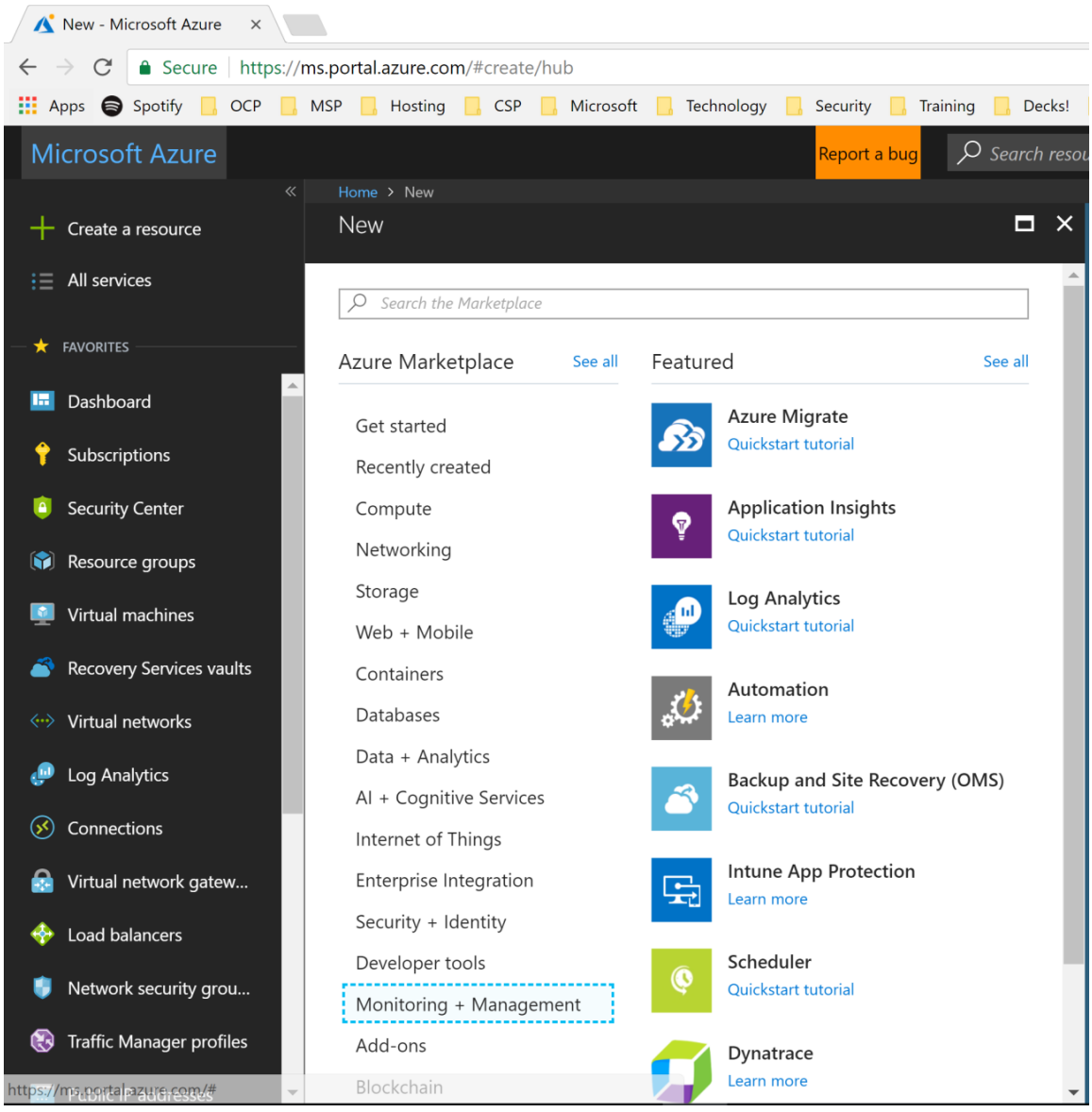
Configuración servicio de replicación

Para efectos de esta guía, se replicará una máquina virtual ejecutándose en un virtualizador Hyper-V hacia la nube de Azure.

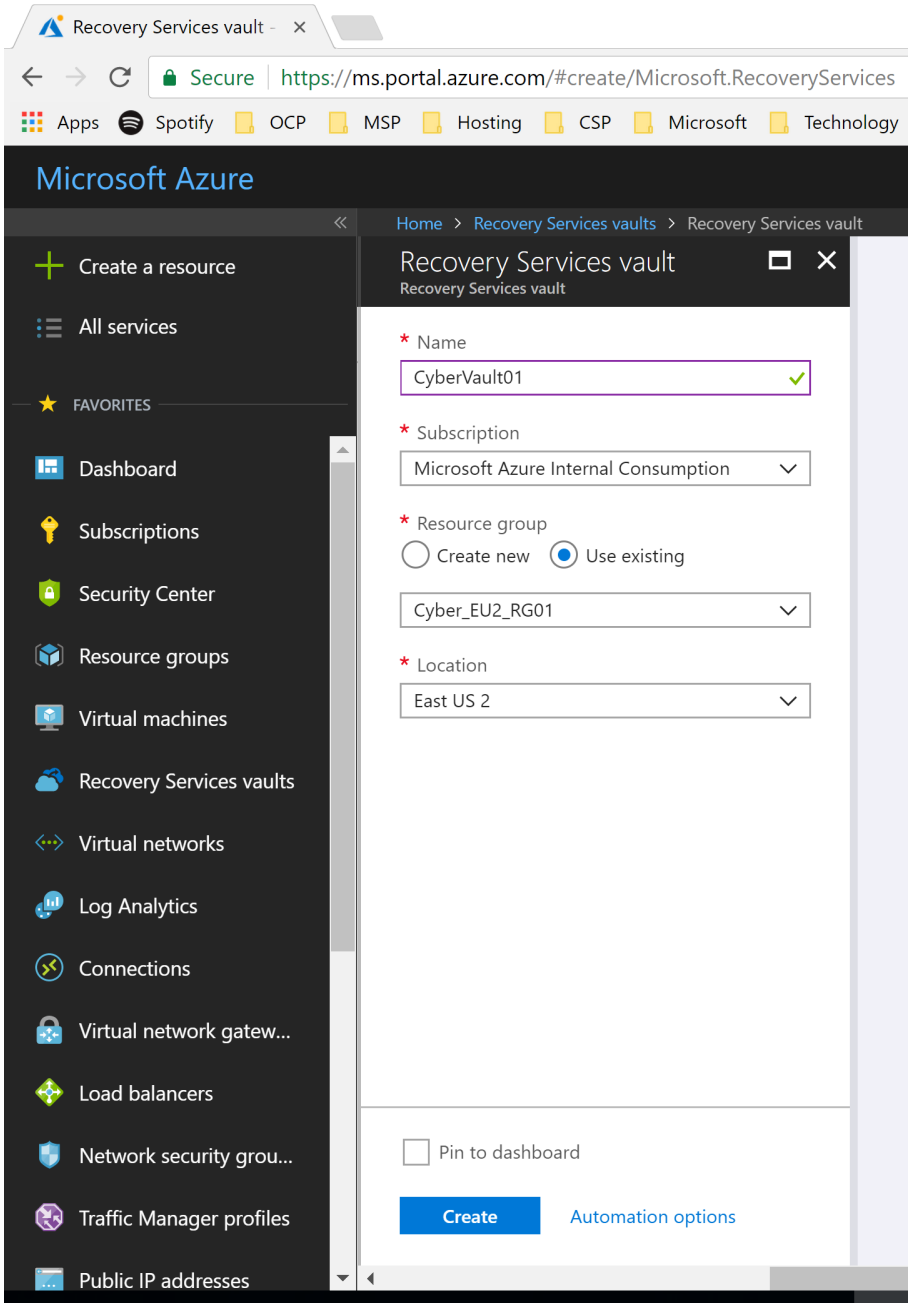
Configuración de la bóveda de replicación y servidor de virtualización

El primer paso es crear la bóveda de replicación, podemos utilizar la misma que se creó anteriormente o bien crear una nueva. Es recomendación del autor crear bóvedas separadas para respaldos y para replicación de servidores, esto por temas de separación lógica y de control sobre las mismas. Para efectos de esta guía utilizaremos la misma bóveda, aunque el proceso de creación es idéntico y sencillo cada vez que se crea una bóveda, se detalla a continuación.

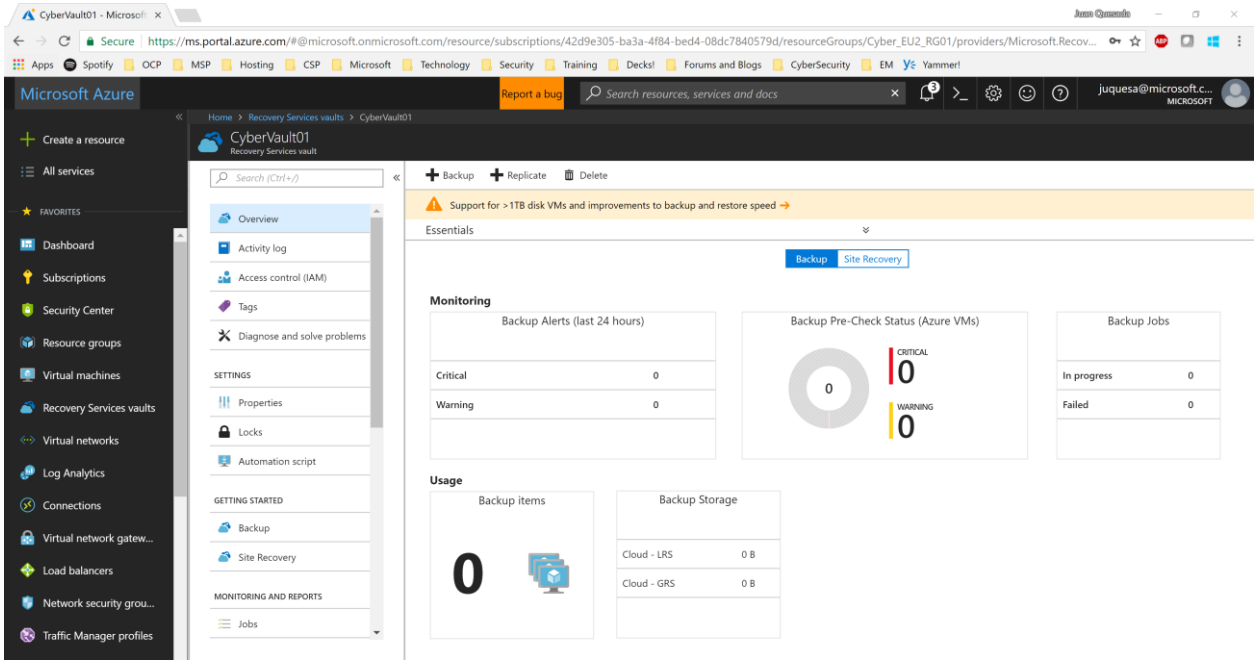
Para crear la bóveda debemos tener una suscripción disponible, ya sea comprada por la página web o algún socio vendedor, como por ejemplo los proveedores de soluciones Cloud (CSP por sus siglas en inglés). Esta bóveda es donde se almacenarán los datos de manera encriptada. Para crear la bóveda, navegamos dentro de https://portal.azure.com, en la esquina izquierda superior buscamos “create a resource”, navegamos a “Monitoring + Management” y damos click en backup and site recovery.



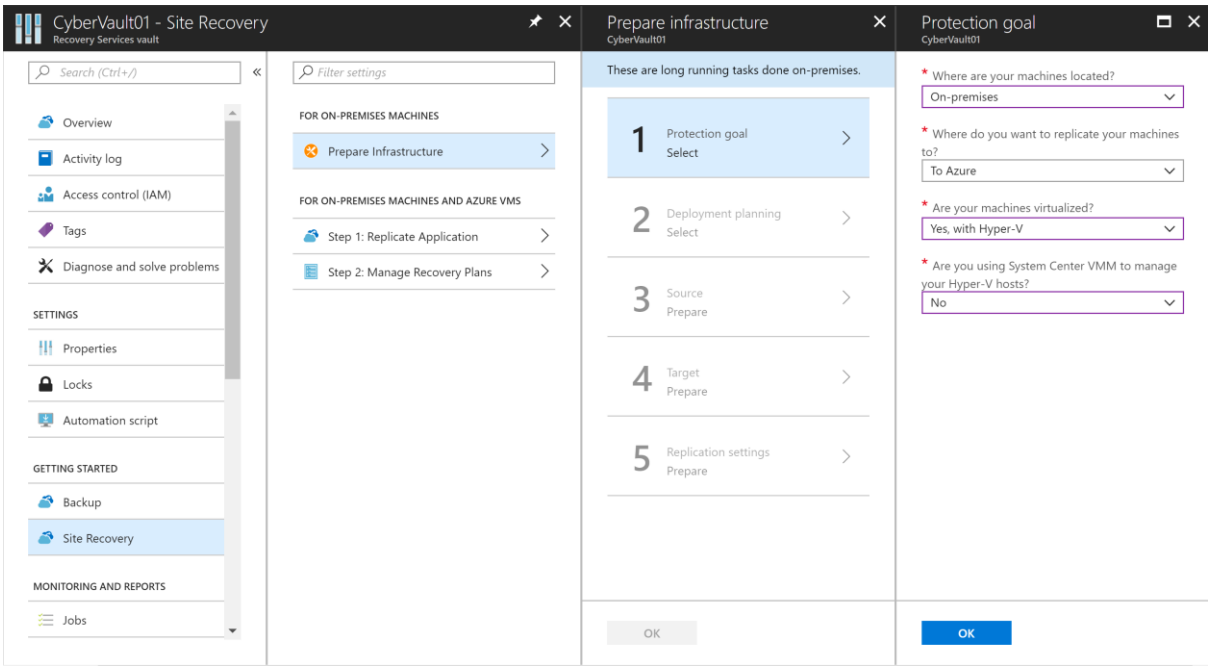
Completamos la información solicitada, le ponemos un nombre a la bóveda, seleccionamos la suscripción, así como el centro de datos a usar.



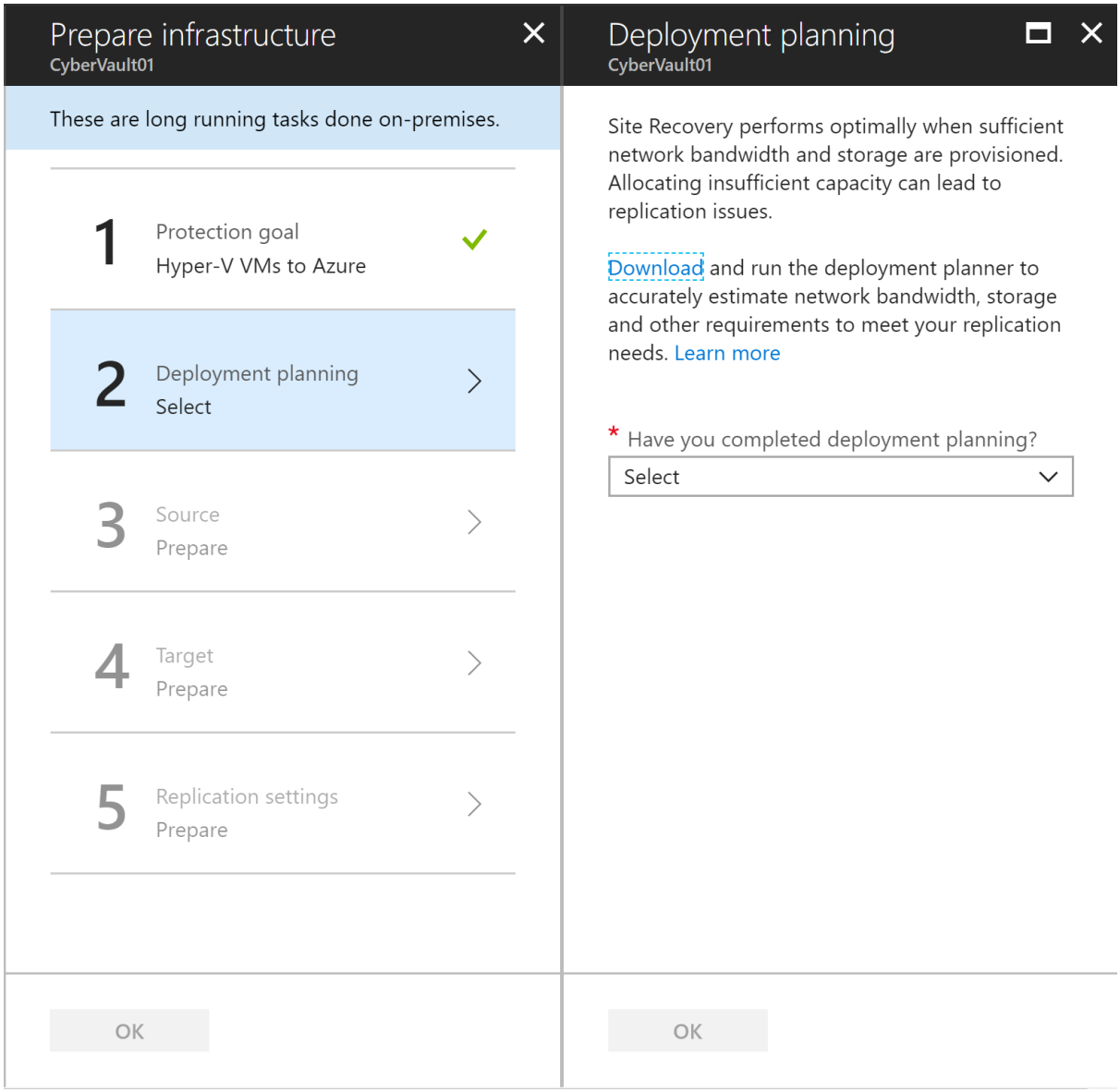
Pocos segundos después la bóveda estará creada, se debe mirar como en la imagen.



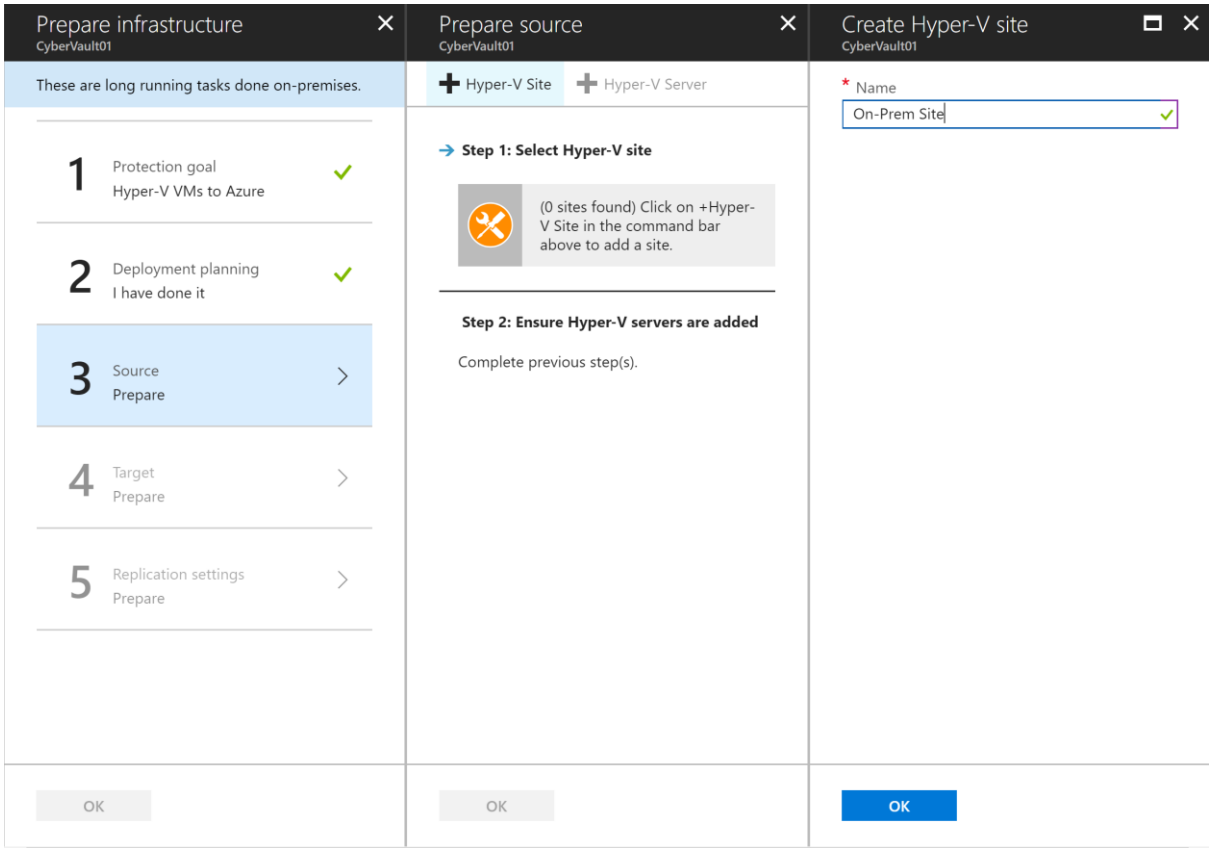
Paso 1: Ya por creada la bóveda, navegamos a getting Started, site recovery, seleccionamos prepare infraestructure y en protection goal escogemos nuestro escenario. Esta guía como se comentó muestra el escenario de una máquina virtual en un centro de datos local (on-premises) replicado a Azure con tecnología de virtualización Hyper-V sin manejador System Center VMM.



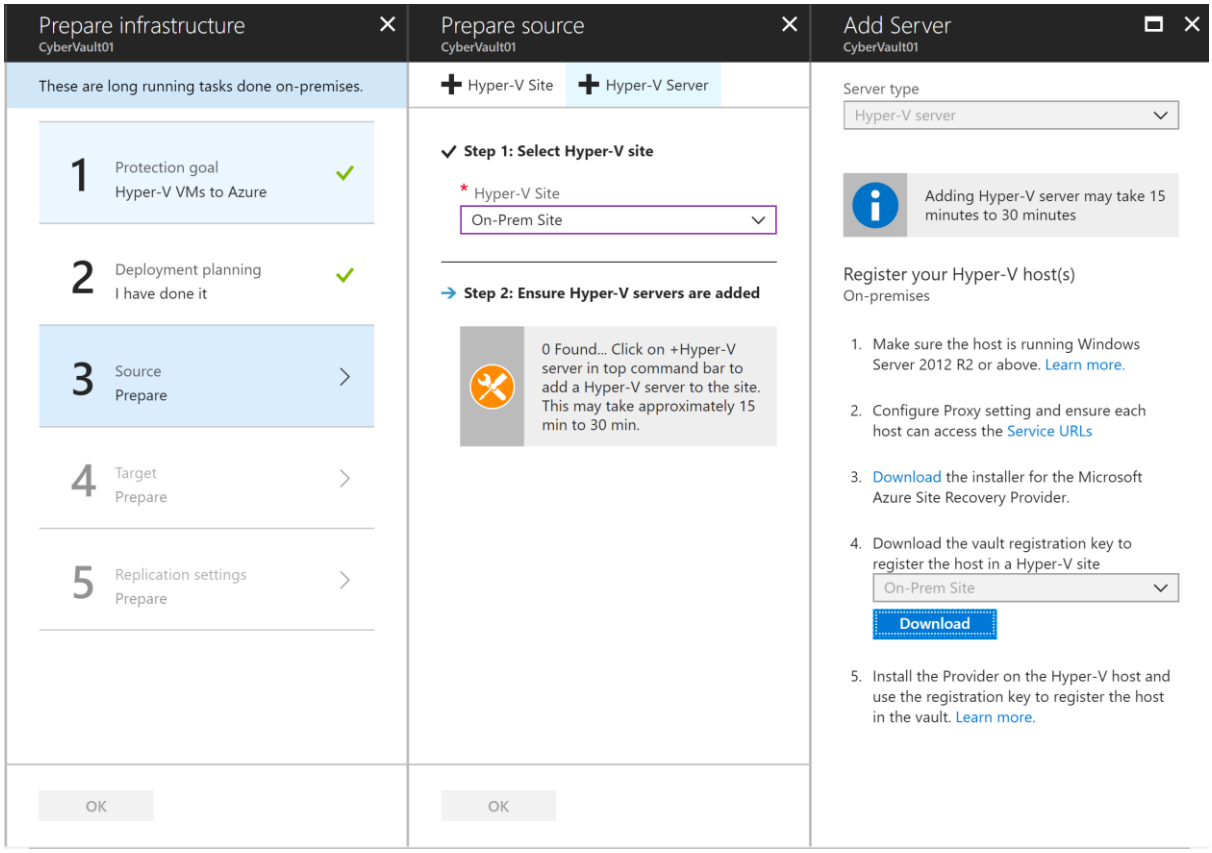
El paso siguiente a ejecutar es opcional, aunque es altamente recomendado. Se trata del planeador de capacidad o deployment planner, el cual nos dará recomendaciones de cuánto almacenamiento, ancho de banda y recursos se requieren para ejecutar una implementación adecuada y mantener la replicación de manera saludable.



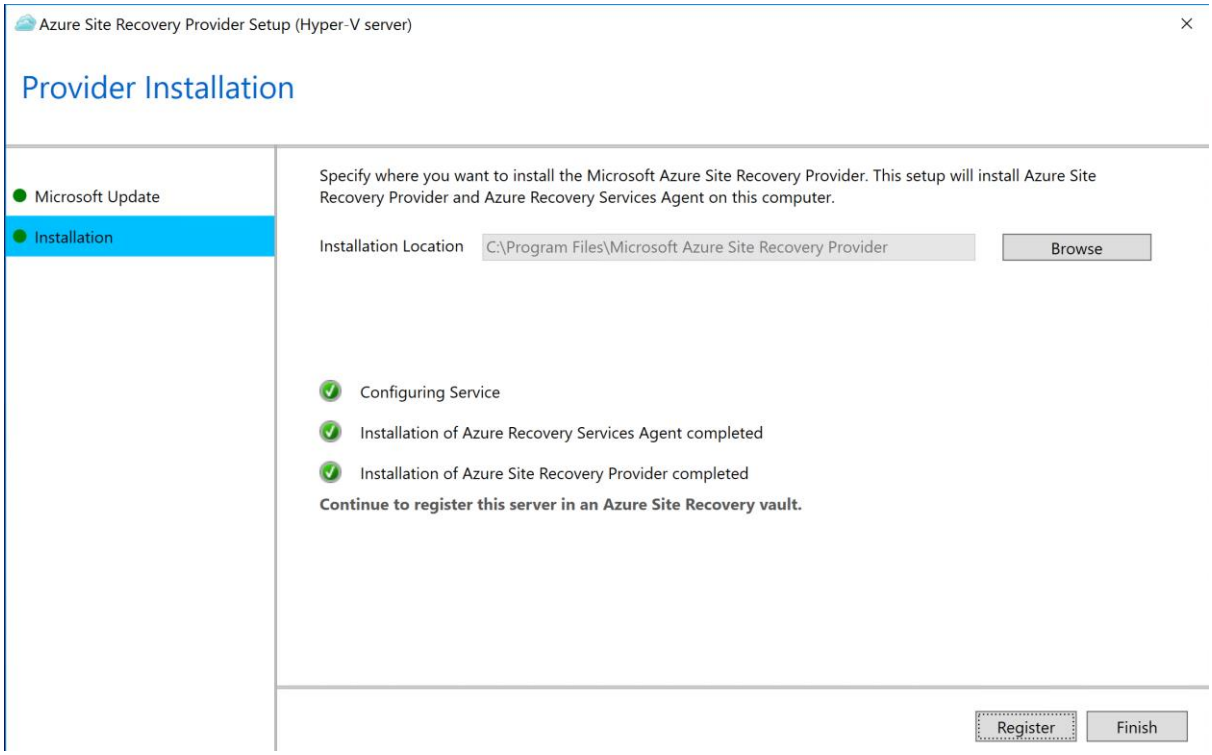
Paso 2: Creamos el sitio de Hyper-V el cual es un nombre lógico de la referencia de un centro de datos.



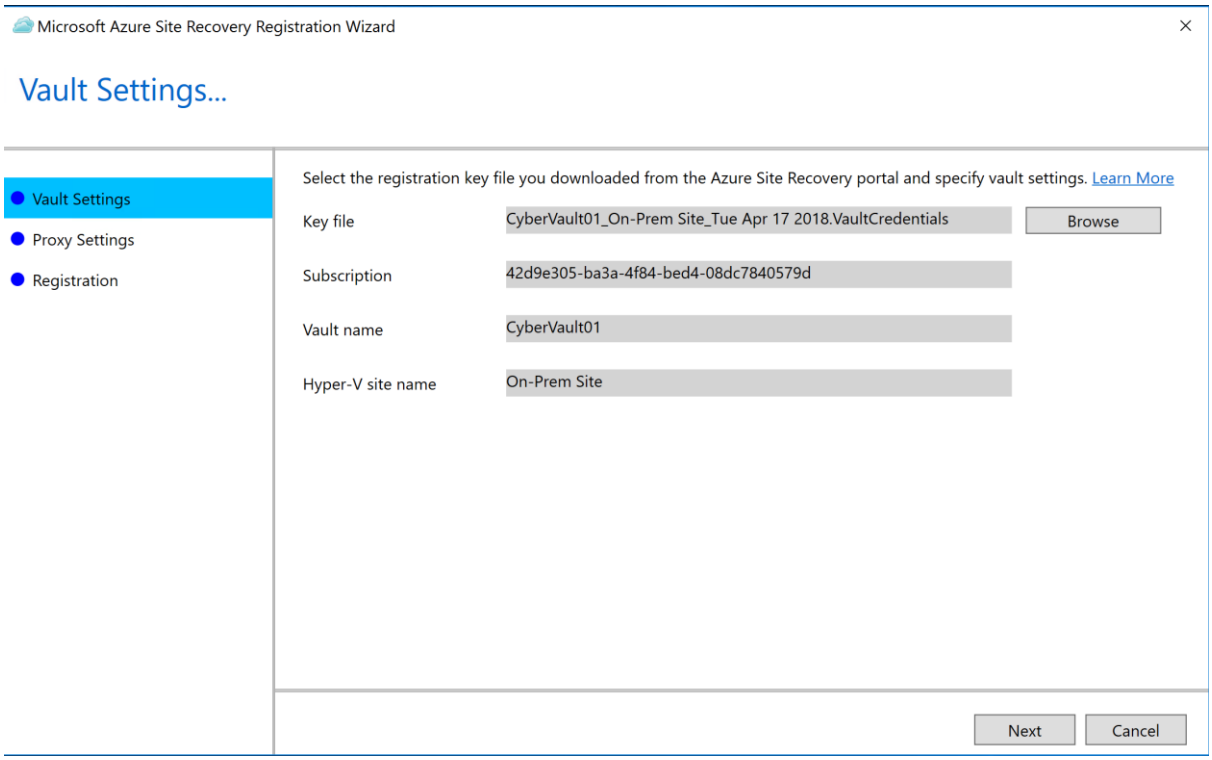
Paso 3: Luego de creado el sitio, agregamos el servidor de Hyper-V. Para esto debemos descargar el agente de replicación a Azure, el cual es un ejecutable que debemos descargar e instalar en los servidores Hyper-V. De igual manera debemos descargar las credenciales que las cuales contienen la conexión hacia la bóveda de Azure.



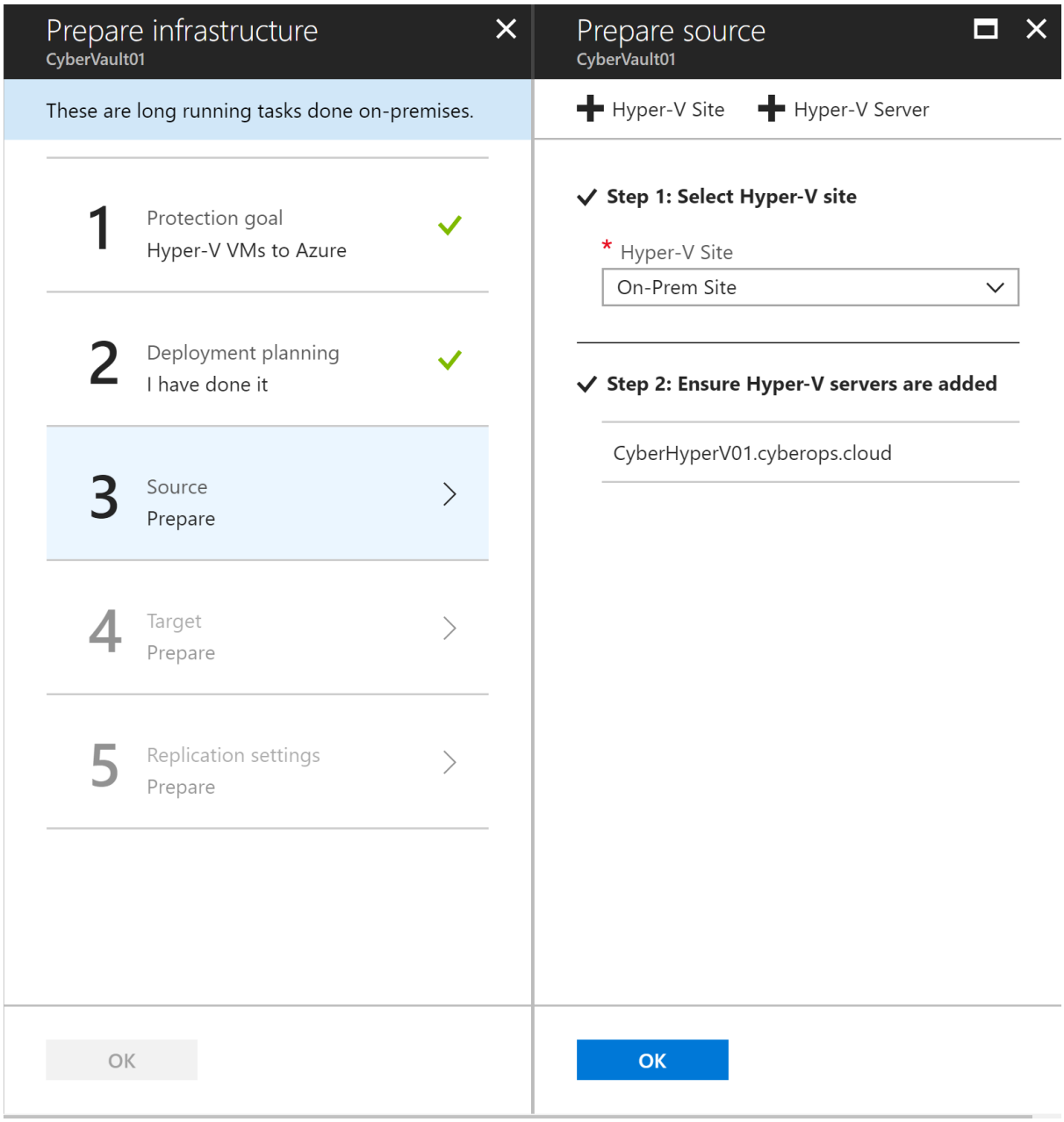
La instalación es bastante sencilla, solamente ejecutamos el instalador y cuando nos piden seleccionamos las credenciales descargadas.



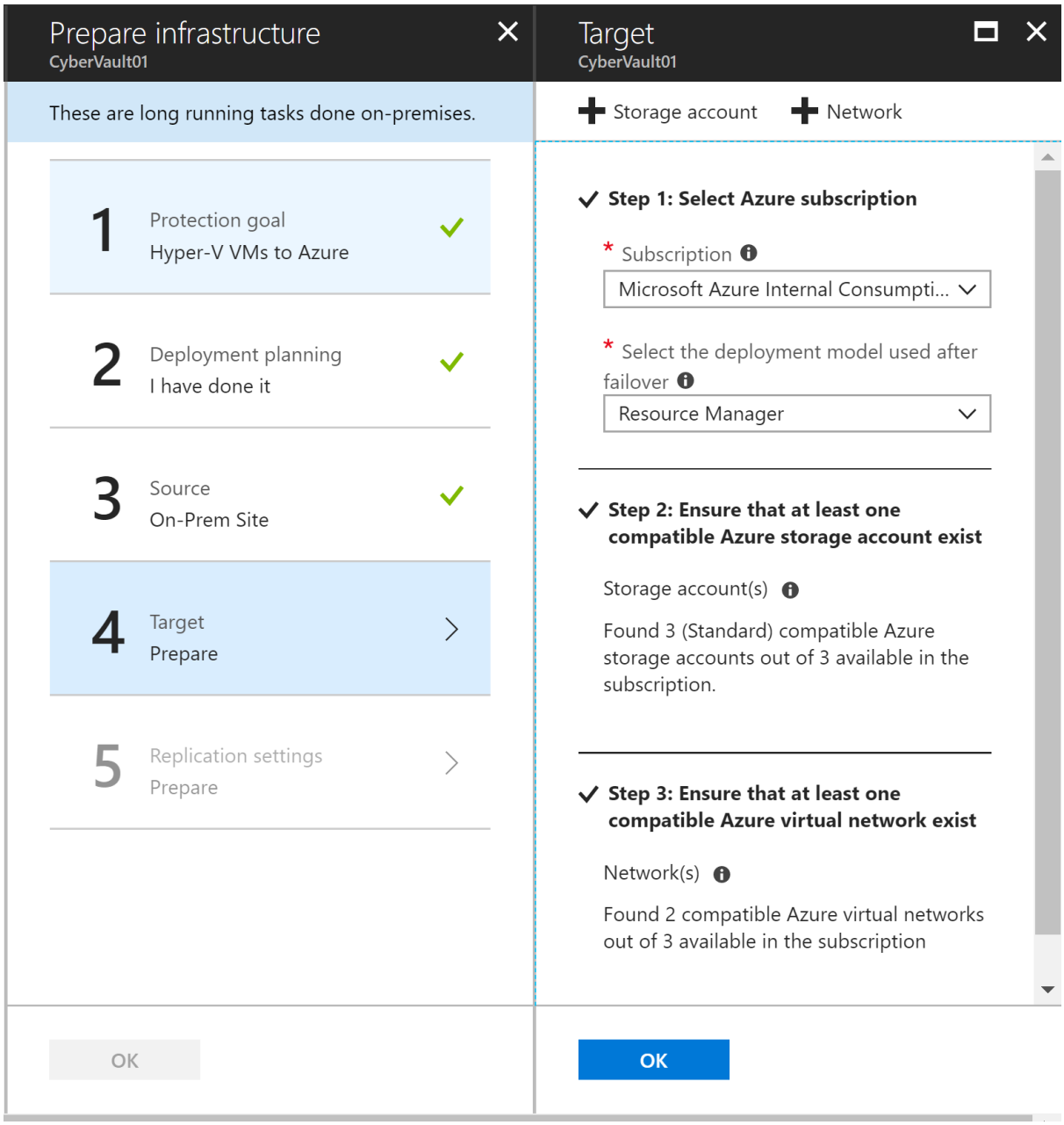
Validamos que la bóveda de respaldos y demás información sea correcta.



Ya por instalada volvemos al portal de Azure y continuamos el proceso, como nota es importante refrescar la página web para que aparezcan los servidores agregados.

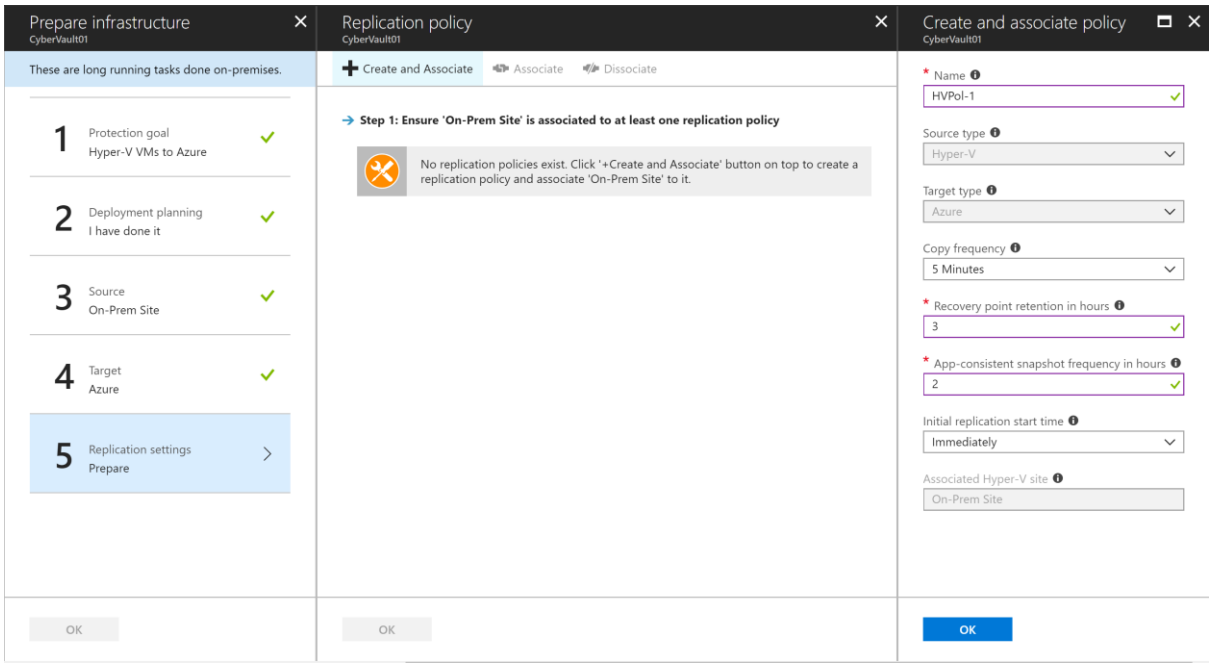


Paso 4: Escogemos la suscripción de Azure, así como una bóveda de almacenamiento y una red. En caso de no existir alguna se puede crear fácilmente completando la información solicitada en el proceso.



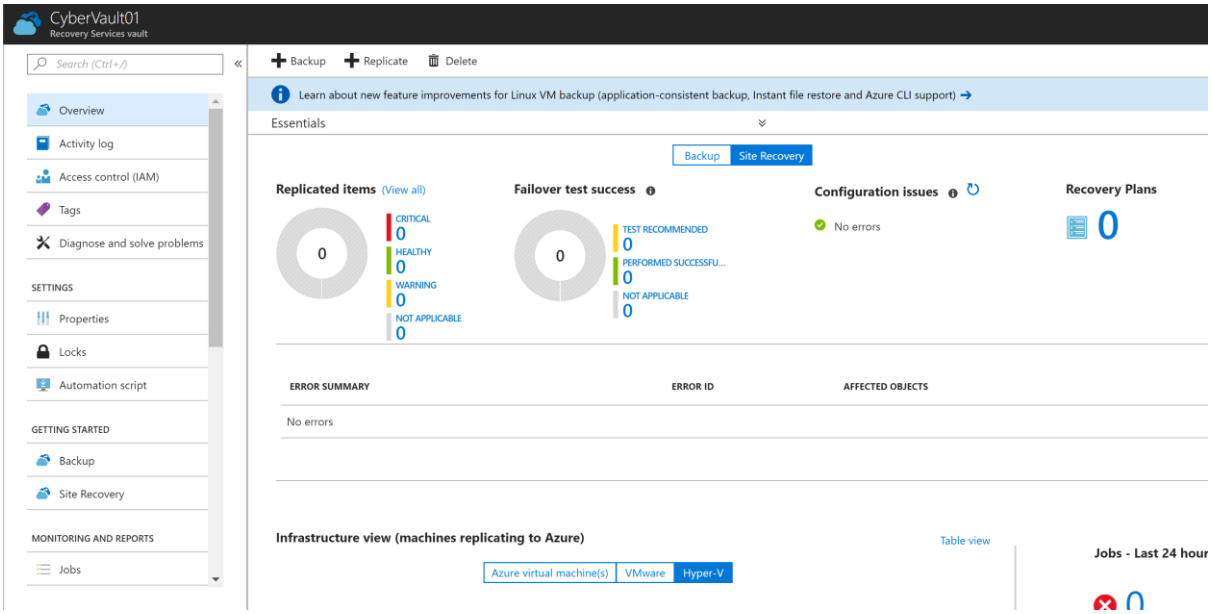
Paso 5: Como paso final de la configuración, seleccionamos o creamos una política de replicación.

- Frecuencia de la copia, es cada cuánto queremos que se sincronice las máquinas virtuales hacia la nube. Para Hyper-V existe un rango entre 30 segundos y 5 minutos. A menor tiempo mayor uso de internet, pero se mantiene la información más reciente.
- Retención del punto de recuperación en horas. Nos permite seleccionar cuánto tiempo guardamos los puntos de restauración. El valor puede ser 0, es decir solo podemos recuperarnos a la última versión o hasta 24 horas.
- Frecuencia Imagen consistente a la aplicación. Señala cuántas imágenes que mantengan consistencia aplicativa queremos por hora.

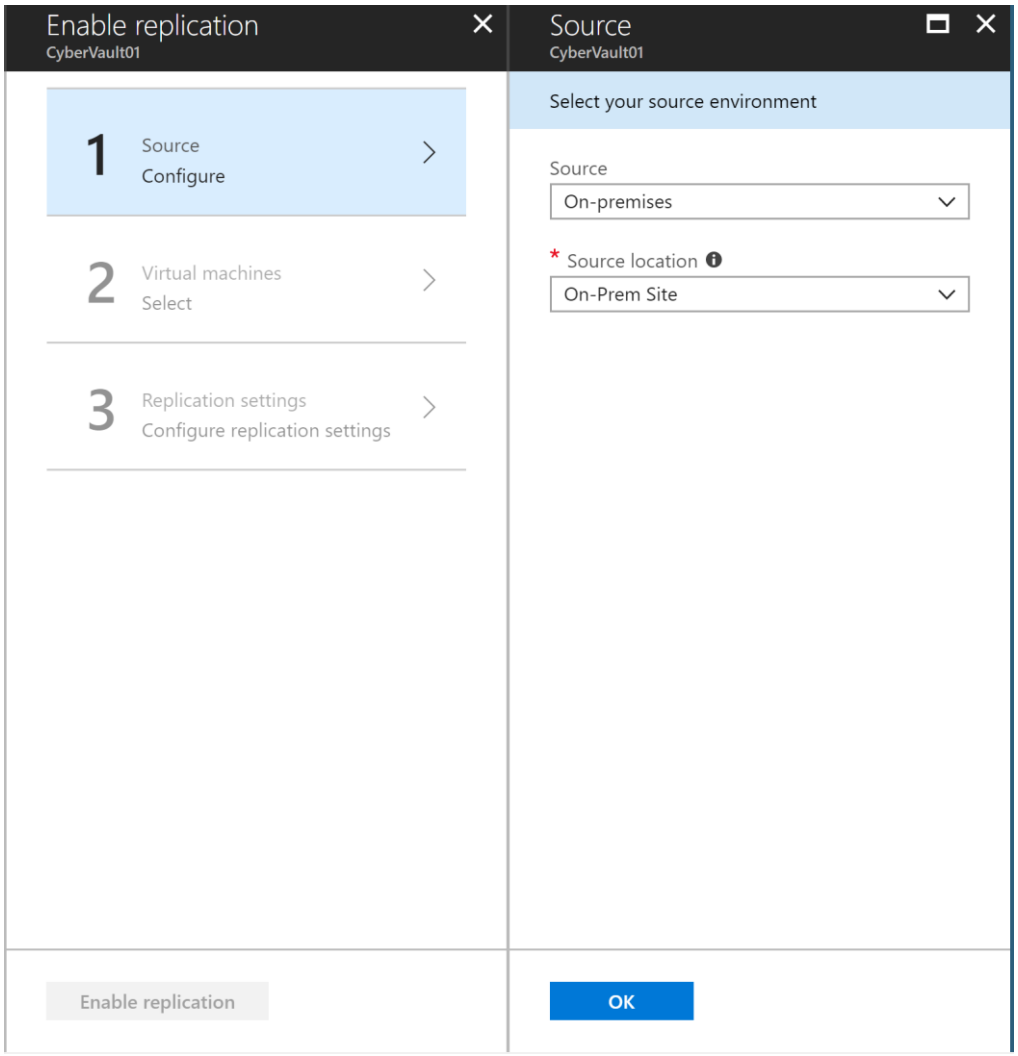


Replicación Máquina Virtual

Luego de configurada la bóveda y de conectar el servidor de Hyper-V a la misma, procedemos a seleccionar y replicar las máquinas virtuales desde el servidor de virtualización hacia Azure. Para esto navegamos en Azure hacia la bóveda de respaldo y le damos clic en replicate.

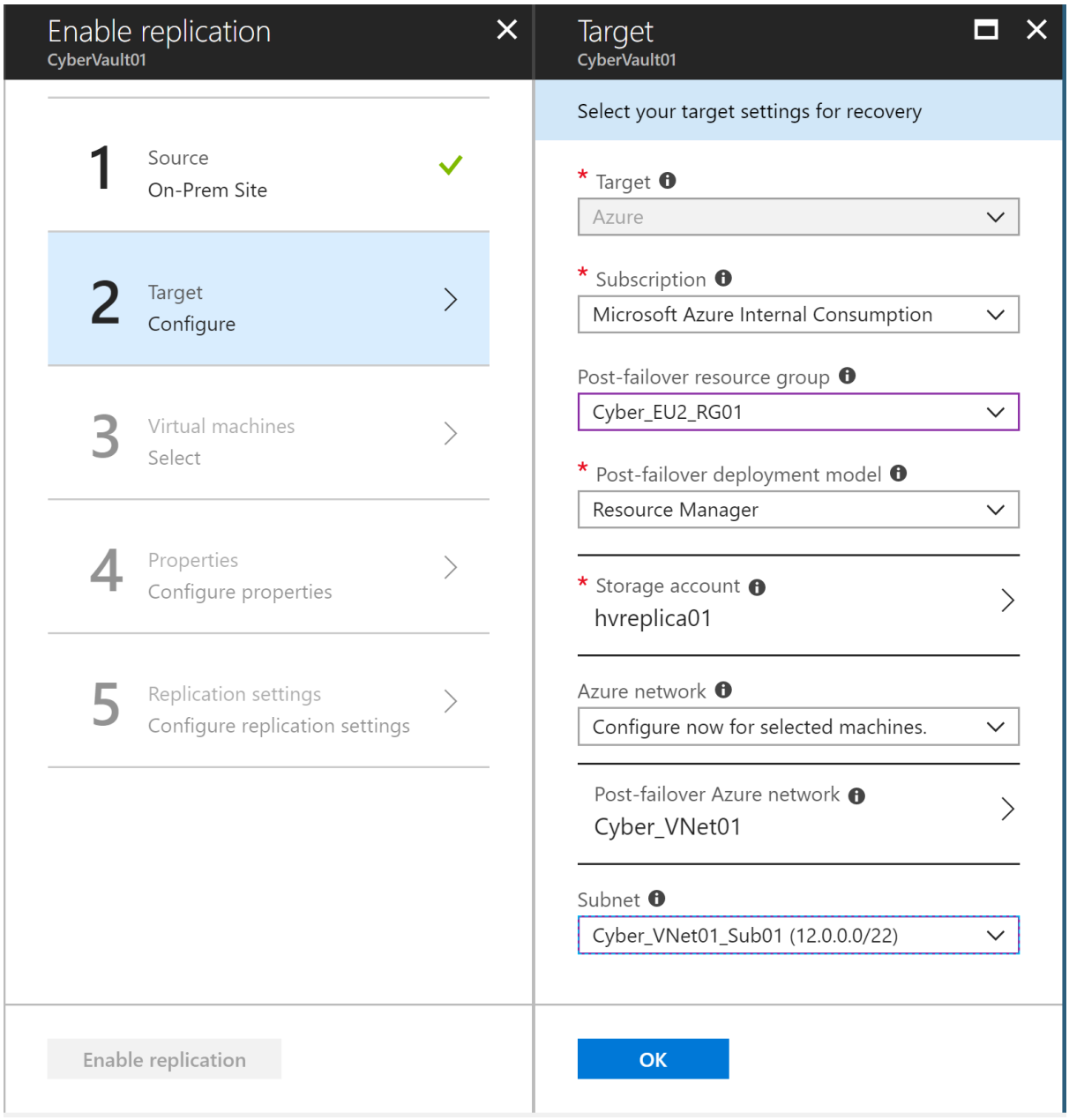


Paso1: Configuramos la ambiente fuente, el mismo fue el que creamos en el proceso anterior.

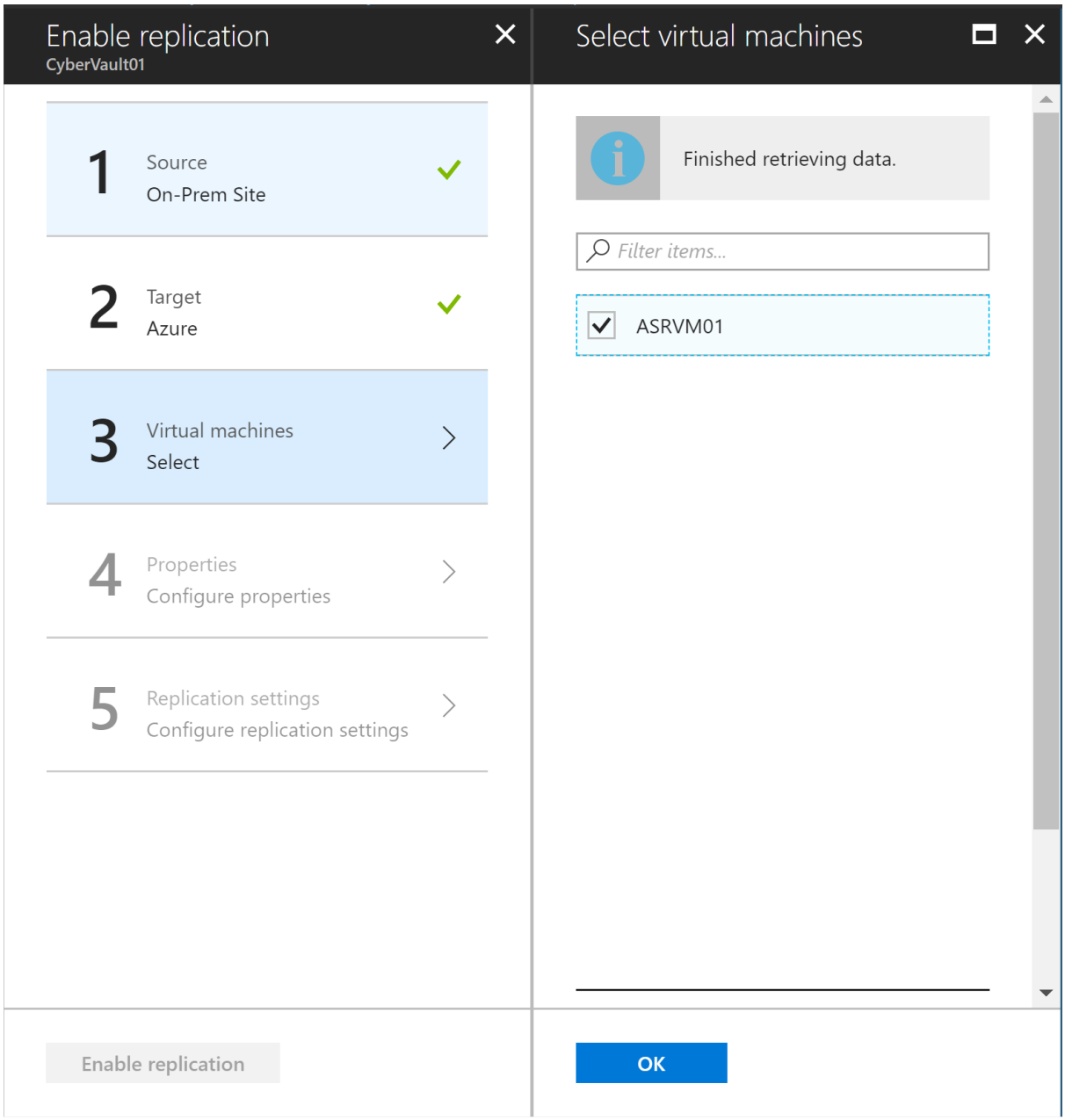


Paso 2: Configuramos las características de replicación.

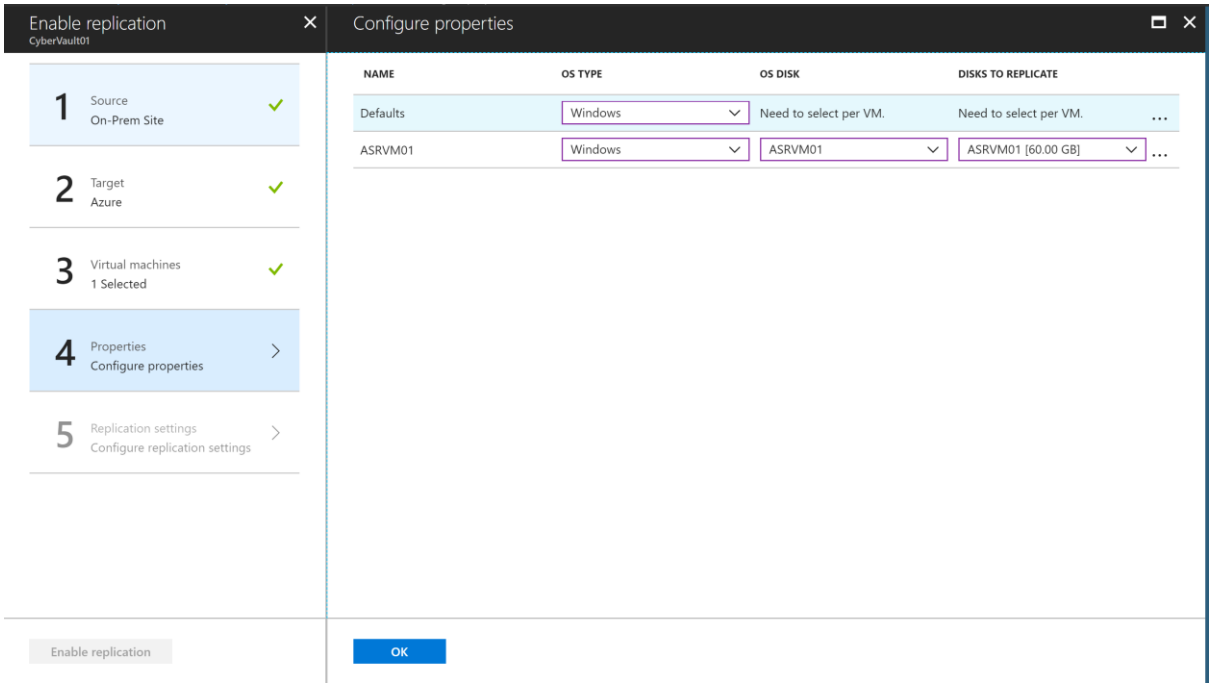
- Suscripción de Azure: Escogemos la correcta dado que puede tenerse varias.
- Resource Group. Agrupación lógica donde pertenecerá la máquina virtual.
- Cuenta de almacenamiento: Bóveda de datos donde se replicarán las copias de los discos virtuales de la máquina virtual.
- Red virtual: Selección de la red donde residirá la máquina virtual en caso de encenderse.



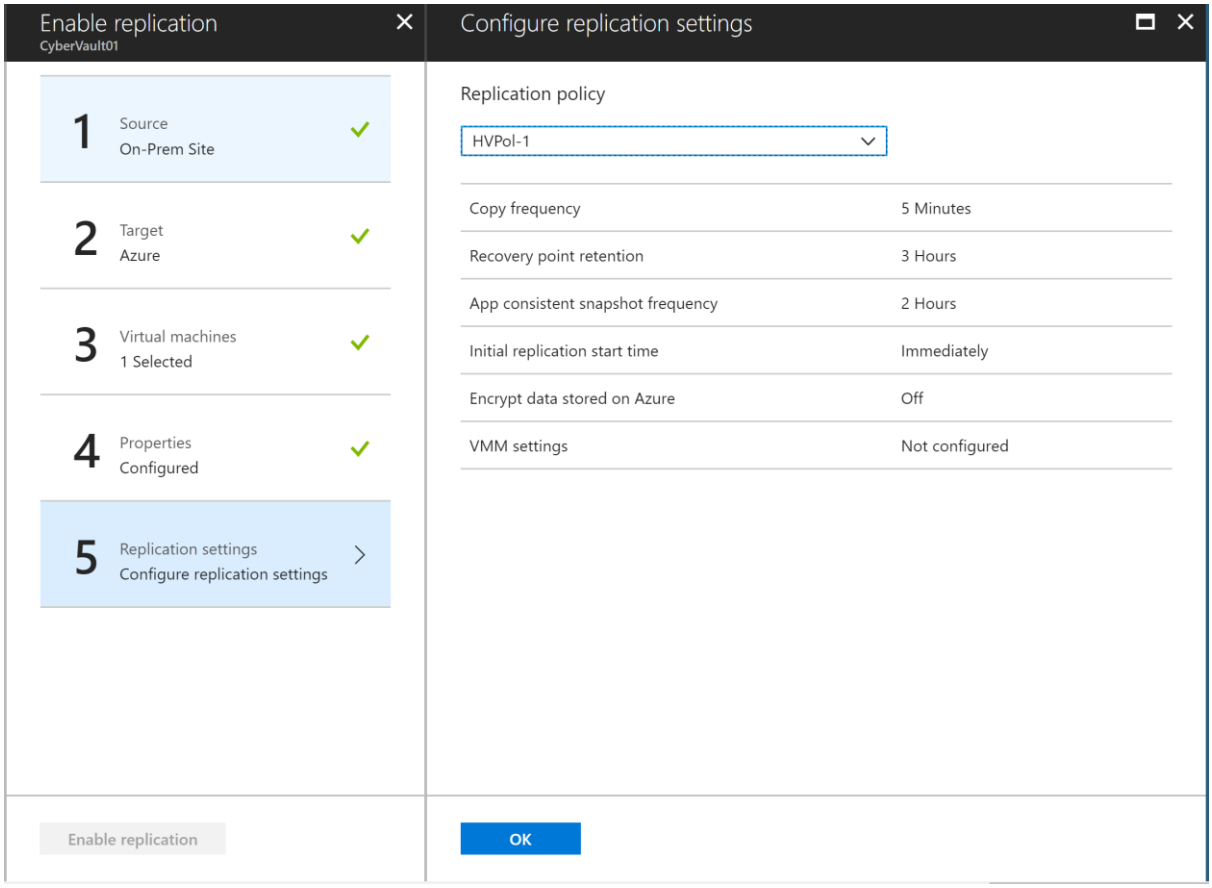
Paso 3: Selección de las máquinas virtuales a replicar, aquí podemos escoger con granularidad qué queremos replicar y qué no. Como se comentó anteriormente, es necesario saber cuáles son las máquinas virtuales críticas y replicar únicamente las que se tienen planeadas en el proyecto. Si la lista es muy grande, se recomienda replicar en pequeños grupos de 3 máquinas para no saturar el enlace de internet. Cada vez que terminen de replicarse las máquinas virtuales volvemos y replicamos adicionales hasta completar las que requerimos.



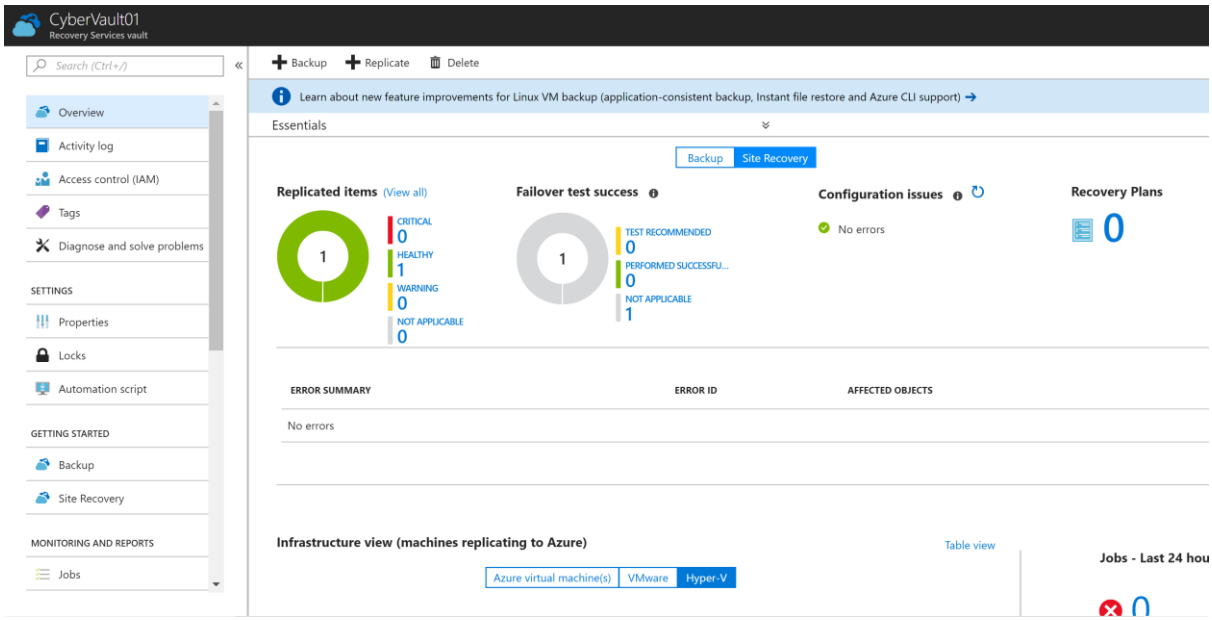
Paso 4: Configuración de sistema operativo y discos. Aquí podemos definirle al sistema cuáles discos queremos replicar y cuál es el sistema operativo que ejecuta la máquina virtual. Aquí de igual manera podemos no replicar todos los volúmenes, aunque esto en su mayoría de veces no es recomendado.



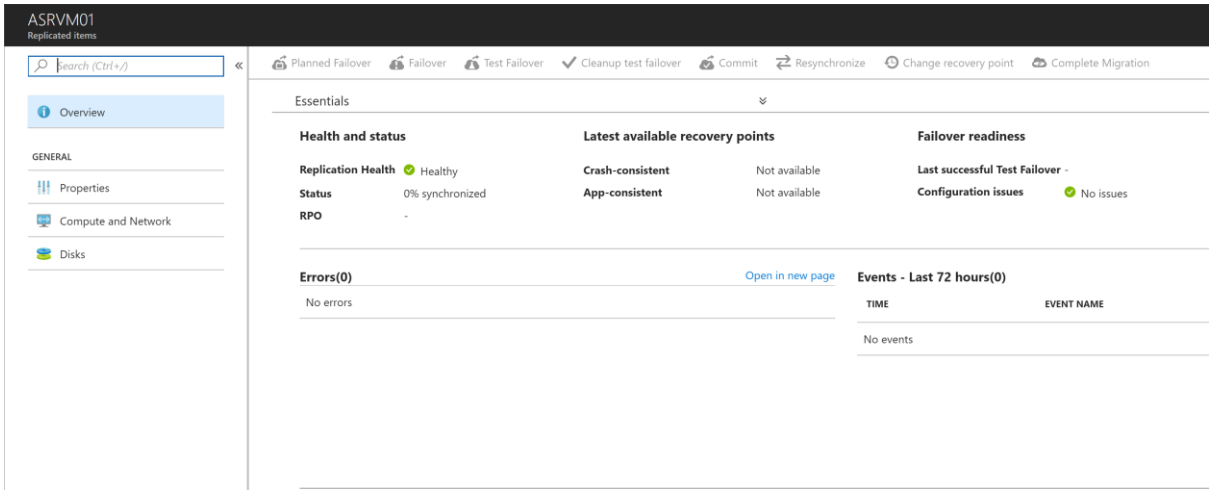
Paso 5: Configuramos la política de replicación que escogimos anteriormente, podemos seleccionar de una lista si tuviéramos más de una. La seleccionada fue la que se creó en el proceso anterior.



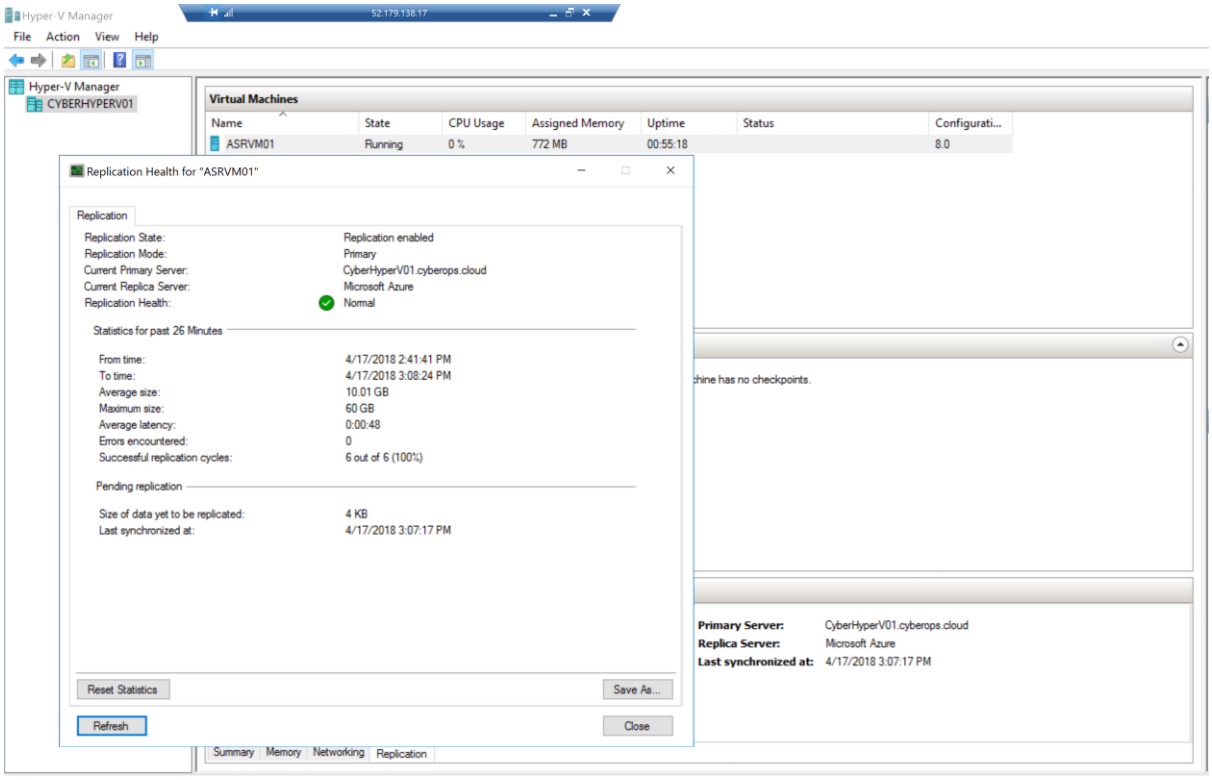
Paso 6: Por último, podemos ir mirando el progreso de la replicación para asegurar se dé correctamente, de igual manera es importante mirar si se da un error y corregir.



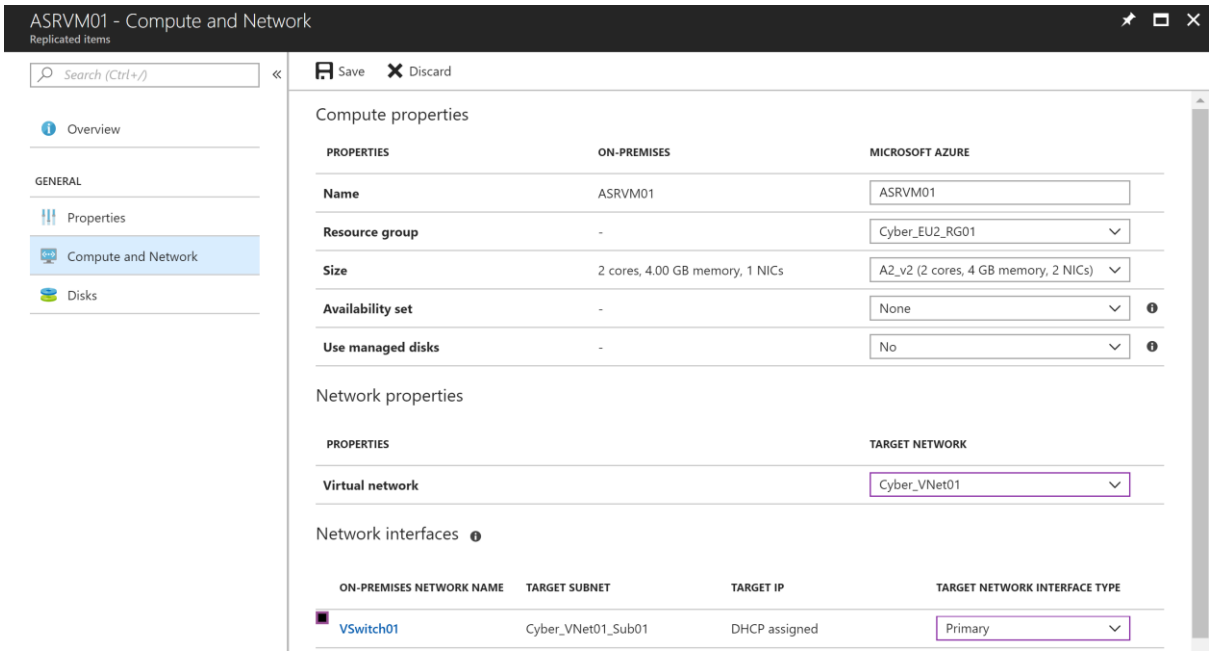
Se recalca la importancia de monitorear para asegurar que la sincronización llegue al 100% sin error.



También desde Hyper-V podemos validar el estado de la réplica desde el Hyper-V manager, en la opción de replicación de la máquina virtual.



Luego de que la replicación se complete, debemos ir a las máquinas replicadas y configurar sus características de recursos que queremos que utilice en la nube de Azure. Si bien idealmente es que tenga la misma cantidad de recursos, podemos seleccionar un tamaño menor para reducción de costos. Aquí mismo escogemos cuál red queremos que la máquina virtual utilice en caso de que tengamos que ponerla en producción.



Con esto, terminamos a la replicación de la máquina virtual hacia la nube y configuramos sus características para funcionamiento.

Como se puede apreciar, tanto para respaldos como para replicación de máquinas virtuales el proceso es sencillo. Creamos las bóvedas adecuadas en la nube, el mismo sistema nos guía a qué tenemos que configurar y qué software tenemos que descargar. Las herramientas de respaldo son bastante intuitivas para un usuario acostumbrado a los respaldos y replicación, y por último podemos estar validando la funcionabilidad desde las herramientas locales o bien desde el portal de la nube que nos dan visibilidad de la salud de las tareas.

Pruebas de los diferentes escenarios de recuperación contra desastres

Restauración de respaldos

En la siguiente parte de este documento se reproducirá pruebas de que los respaldos, así como la réplica de las máquinas virtuales están funcionando correctamente. Es altamente recomendado que, aunque los respaldos no presenten error a nivel de sistema, los mismos se estén comprobando por varias razones:

- Asegura que los datos son funcionales, es decir que en el respaldo no se pierde data por corrupción en el proceso.
- Asegura que los datos son completos, aunque el sistema indique que el respaldo finalizó correctamente podemos correr el riesgo de que sean parciales, porque no se configuraron bien, por algún cambio y no se contempló toda la información como ejemplos.
- Práctica, asegura exista un proceso de práctica donde se restauran los datos, así el equipo está probando los sistemas y los procesos constantemente lo que agiliza la capacidad de reacción ante una eventualidad real.
- Cumplimiento, muchas veces por políticas de empresa o por estándares de industria se requiere validación de pruebas de recuperación contra desastres.

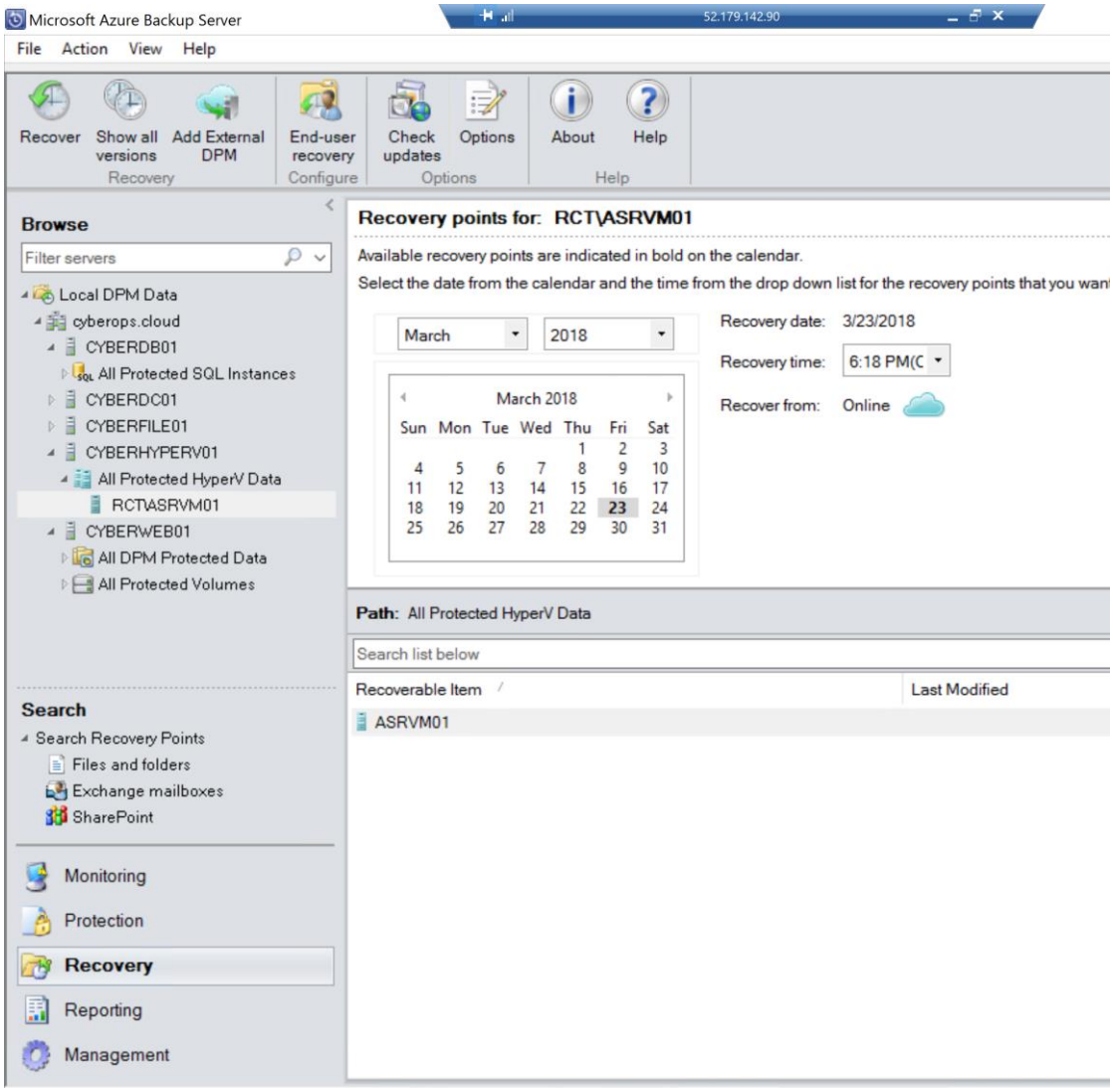
Otra recomendación de crítica importancia es que estos respaldos sean restaurados en equipos no productivos, es decir, servidores dedicados para estos propósitos. Lo anterior dado que, si restauramos como ejemplo, una máquina virtual completa sobre el mismo equipo de virtualización este va a destruir la original y afectar la producción. Dos opciones surgen acá, la primera que el ambiente en sitio tenga capacidad para tener estos servidores, los cuales en su mayoría de tiempo pueden estar apagados para que no compitan

constantemente por recursos de los servidores operativos, o bien pueden utilizarse servidores en la nube para tal fin.

Si la primera opción es posible, es decir hay capacidad suficiente, la misma tiende a ser la más costo-efectiva porque ya se cuentan con los recursos pagos para hacerlo. En caso de que no se cuente con los recursos la nube puede ser muy costo-efectiva al únicamente tener que pagar cómputo por el periodo de la prueba y se deja de pagar cuando los equipos se apaguen; el único cobro en la nube sería el almacenamiento de la máquina virtual apagada, el cual, como vimos en ejercicios anteriores, es de pocos dólares.

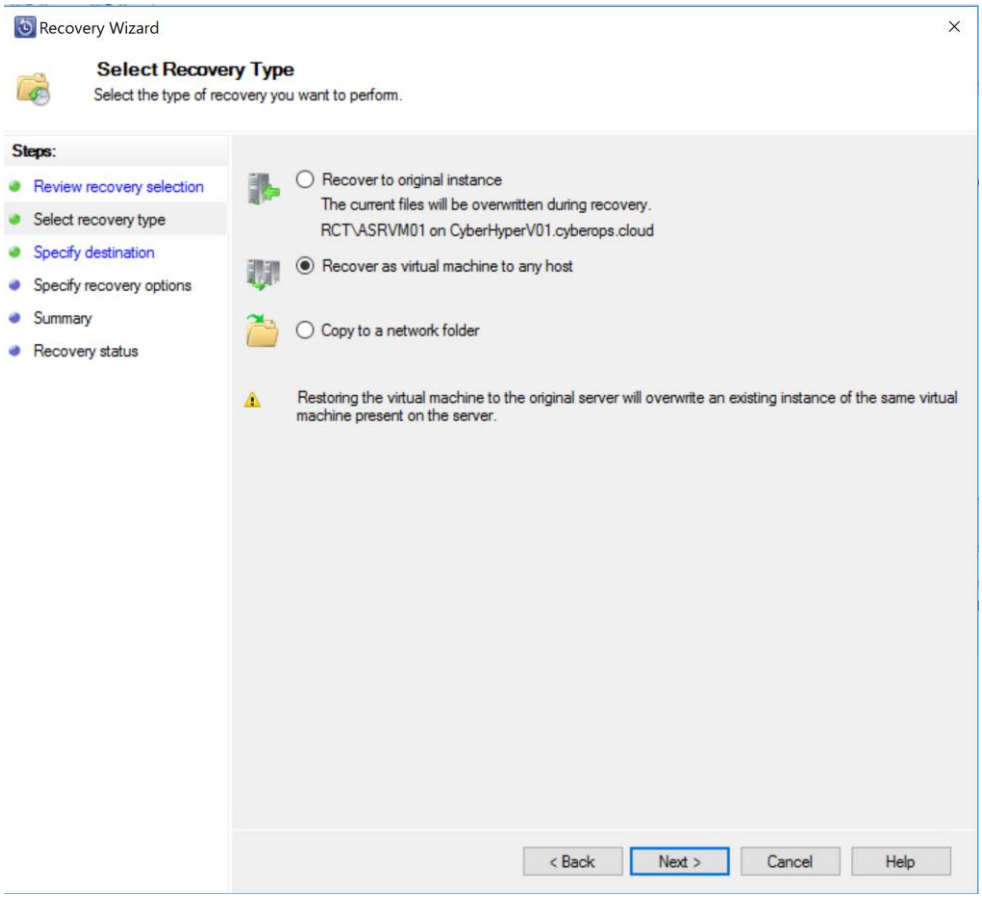
Restauración servidor de virtualización

Desde la herramienta de respaldos, navegamos a recovery y buscamos el servidor de virtualización, al expandir su configuración nos mostrará el inventario de equipos que tiene respaldados; aquí podemos apreciar al servidor asrvm01 que respaldamos anteriormente. De aquí vamos a tener diferentes opciones de puntos de restauración, tanto por fechas como por origen de los datos. Para efectos de la prueba queremos restaurar desde el sitio secundario, es decir los respaldos desde el Cloud, por lo que buscamos una opción de recover from online.

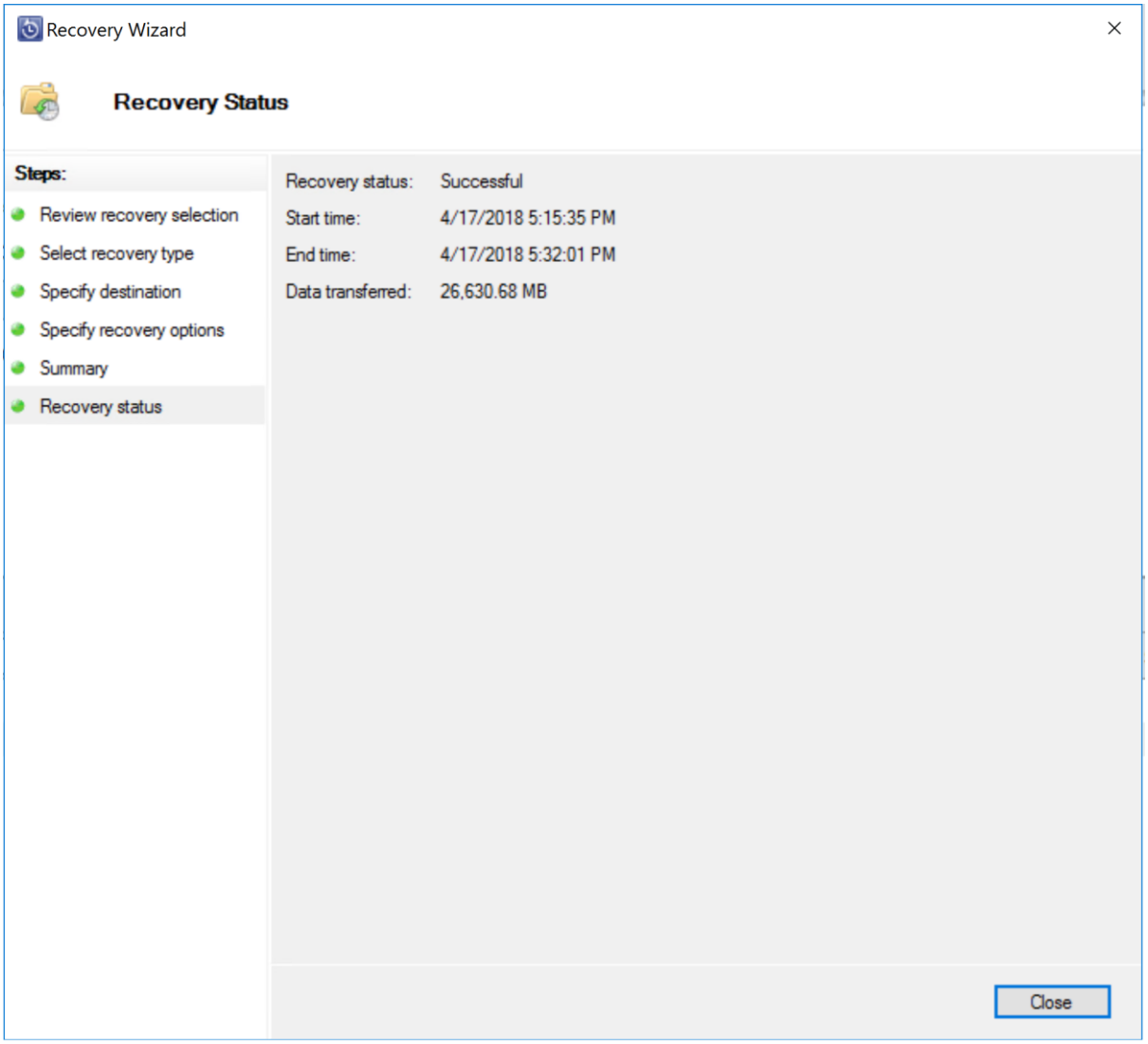


De aquí arrancamos el proceso de recuperación, seguimos las instrucciones básicas y nos detenemos a mirar la opción de dónde restaurar. En un escenario real donde la máquina virtual es irrecuperable, escogemos la primera opción que es recuperar la instancia original, esto rápidamente nos permite volver a producción.

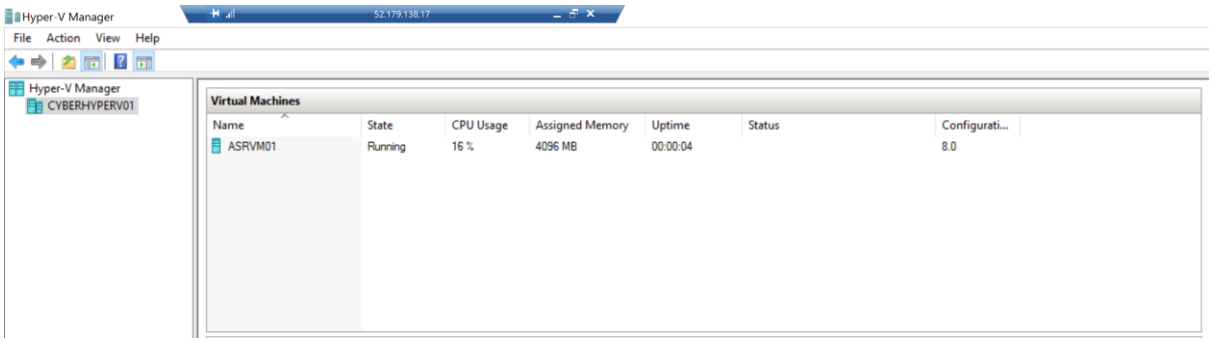
Para efectos de prueba escogemos algún otro servidor de Hyper-v para restaurar la imagen en un ambiente secundario sin afectar producción. Es importante recalcar que si escogemos la segunda opción sobre el servidor productivo donde reside la máquina virtual de producción, el mismo sobre escribe la máquina productiva creando una afectación de servicio, por ende, aseguremos que si es prueba sea en un servidor que no pertenece a producción. Una alternativa es no crear una máquina virtual sino restaurar sus archivos en un folder, si bien la misma permite acceder los datos no lo hace fuera de línea, es decir como archivos.



Luego de terminar podemos comprobar por el mensaje de finalización.

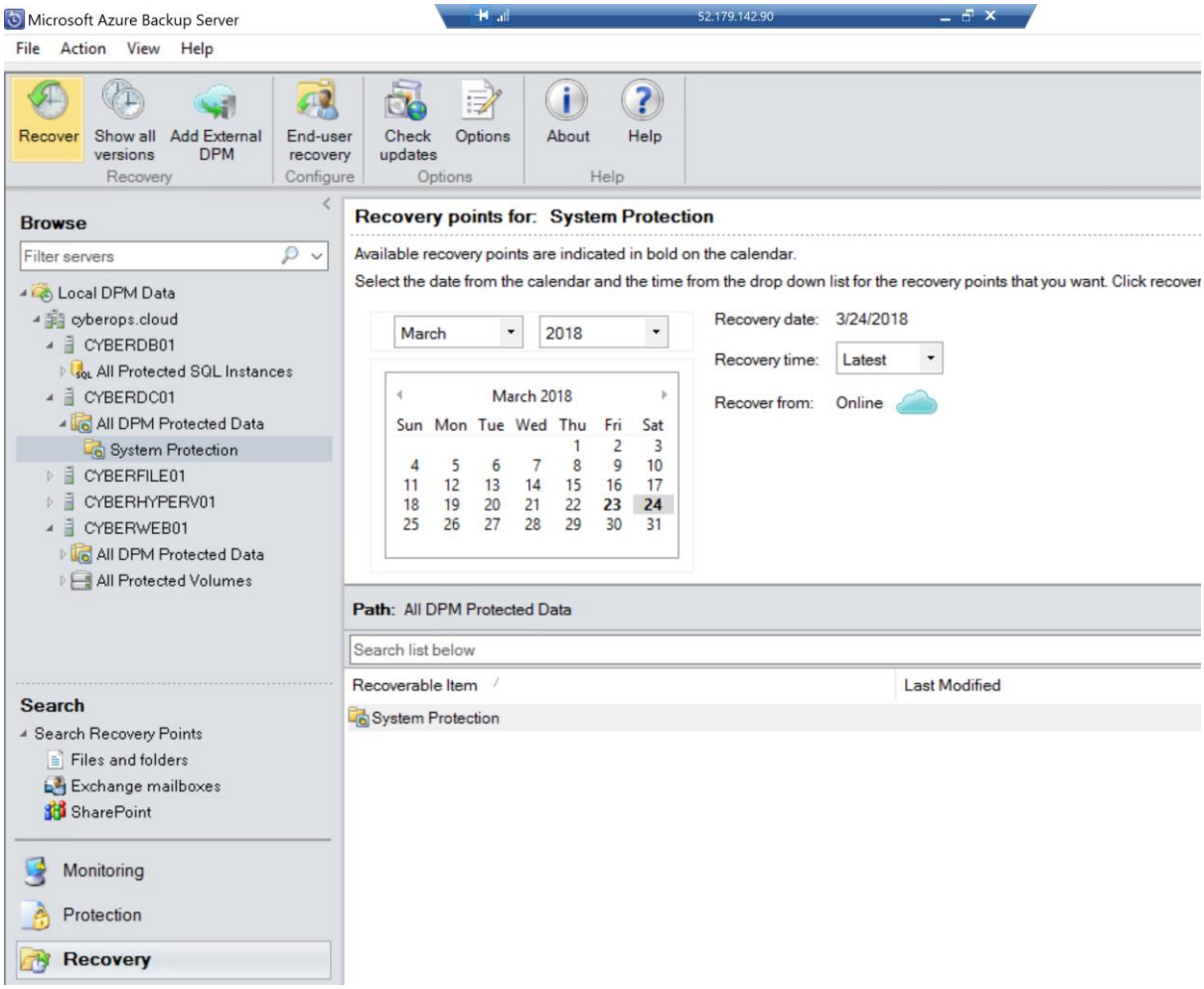


Por último, se puede apreciar la creación de la máquina virtual y que la misma se encuentra operativa, podemos acceder a ella igual como lo hacemos en la ambiente producción y validamos sus datos y función aplicativa. Posterior a la prueba se elimina la máquina virtual normalmente a través del hipervisor.

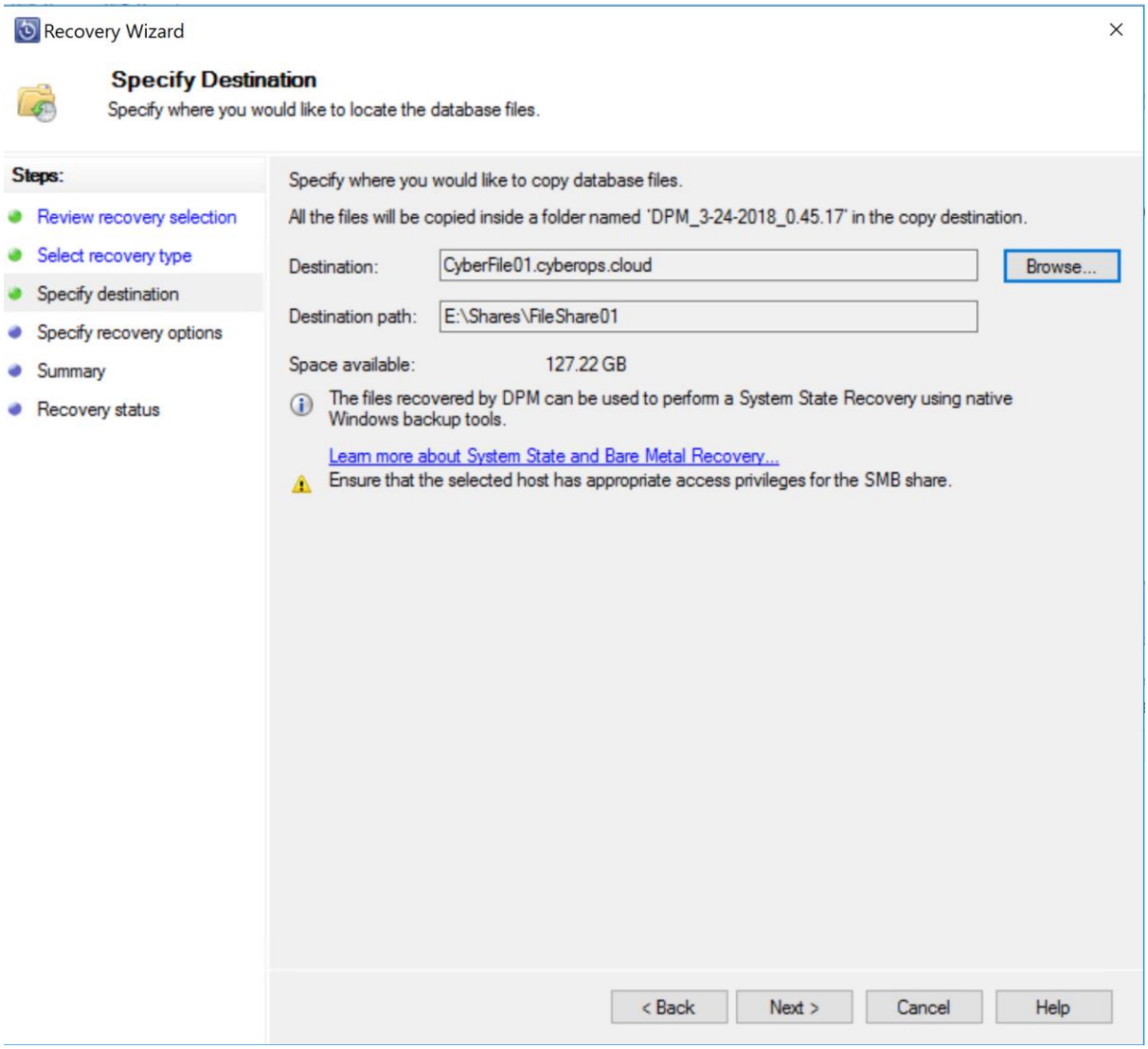


Restauración controladora de dominio

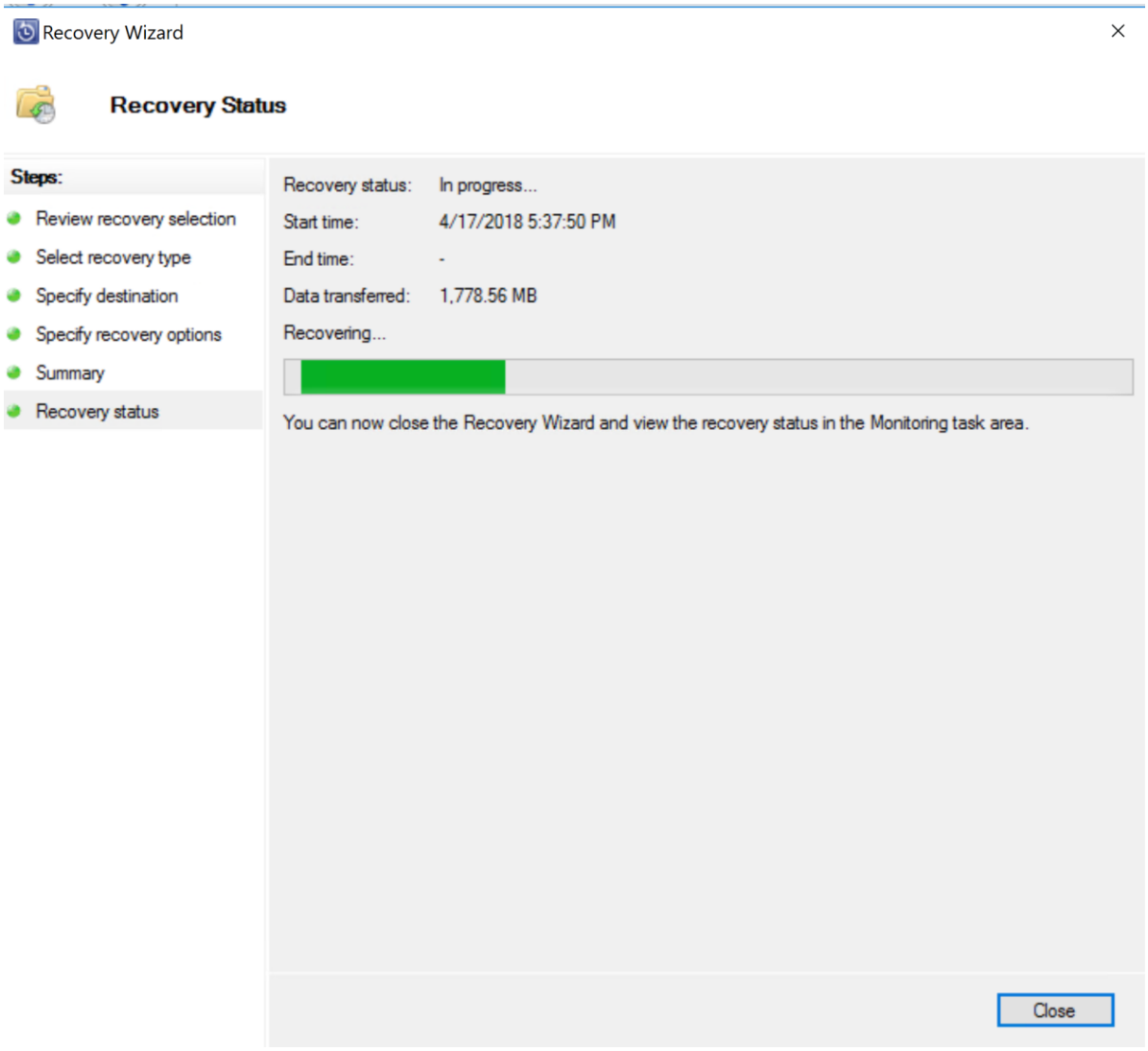
Desde la herramienta de respaldos, navegamos a recovery y buscamos el servidor de virtualización, al expandir su configuración nos mostrará el inventario de equipos que tiene respaldados, aquí podemos apreciar al servidor cyberdc01 que respaldamos anteriormente. De aquí vamos a tener diferentes opciones de puntos de restauración, tanto por fechas como por origen de los datos. Para efectos de la prueba queremos restaurar del sitio secundario, es decir los respaldos desde el Cloud, por lo que buscamos una opción de recover from online.



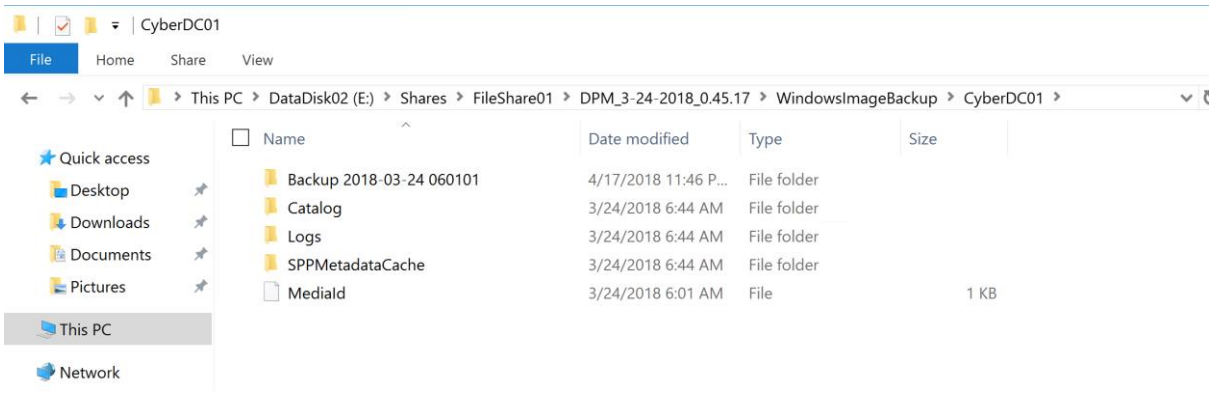
El respaldo del controlador de dominio únicamente permite recuperar a un folder, esto dado que recuperar un controlador de dominio tiene un proceso específico llamado “active directory restore mode” en donde ponemos al servidor en un estado dedicado de recuperación. Esta prueba no realiza dicha restauración porque el objetivo es tener la información disponible desde la nube, no restaurar el mismo. Para recuperarse se recomienda seguir procedimientos oficiales que se encuentran publicados en línea.



Una vez terminada la recuperación, procedemos a validar los datos que fueron depositados en la carpeta seleccionada. Estos son los datos suficientes para realizar la restauración.

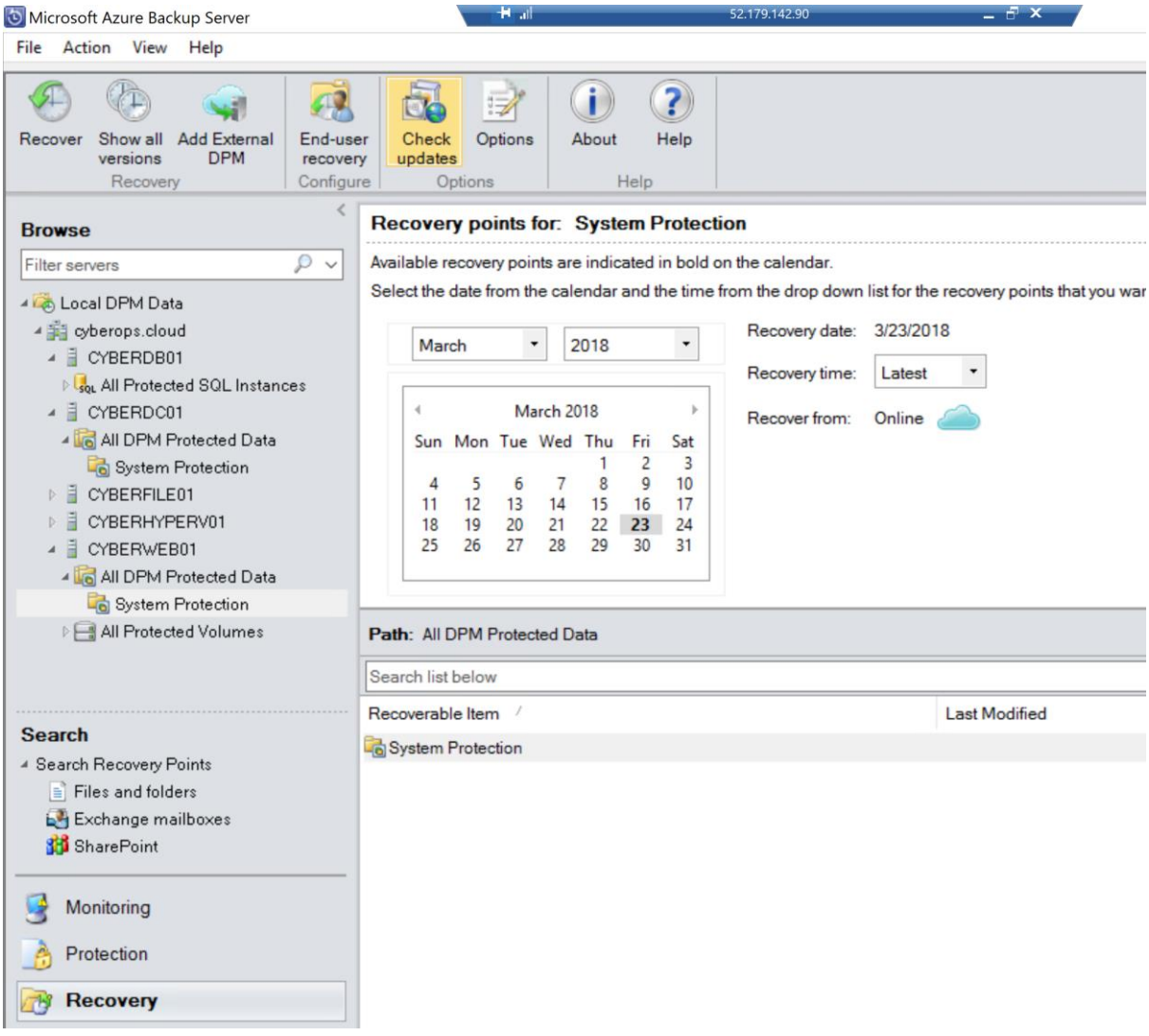


Se verifica la información se restaure en el lugar adecuado.

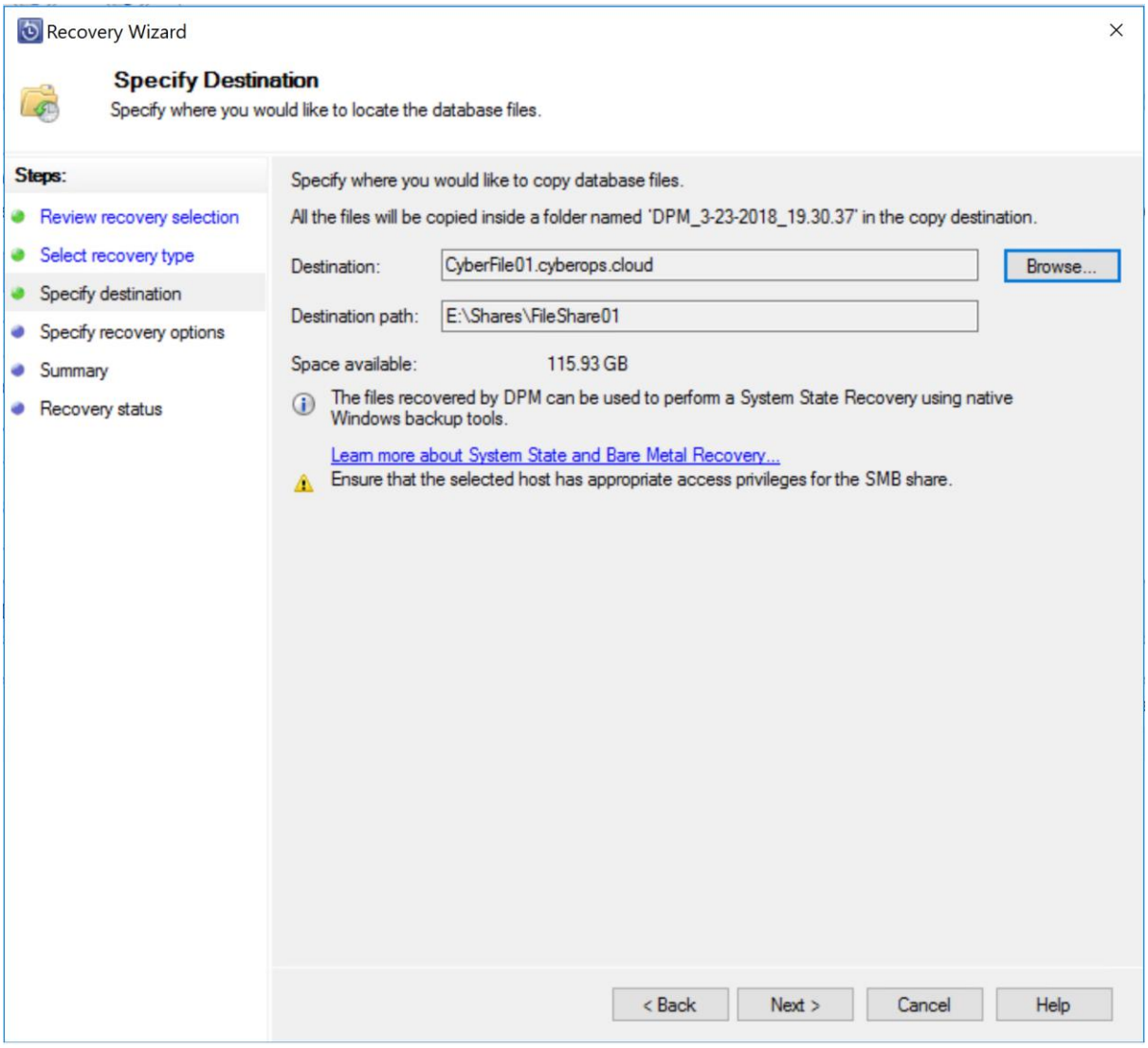


Restauración servidor web

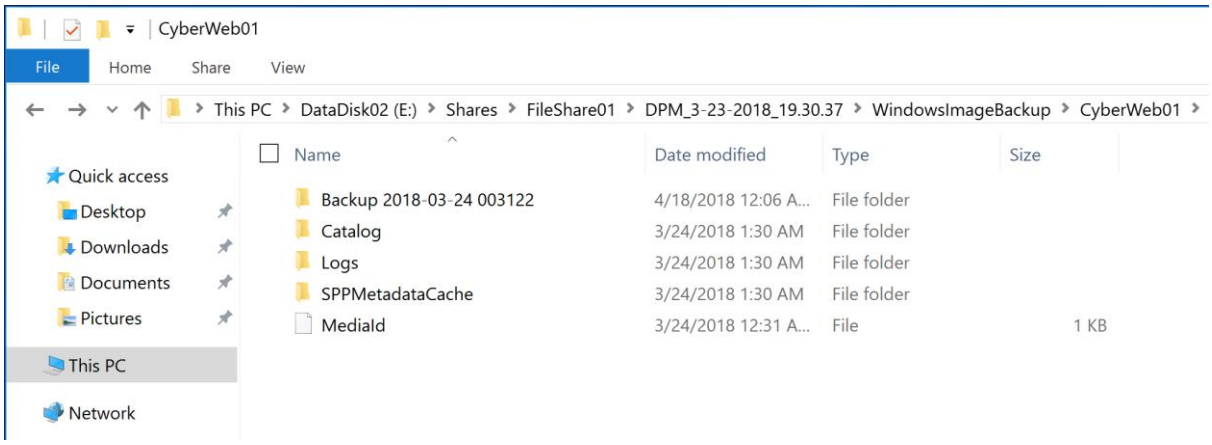
Desde la herramienta de respaldos, navegamos a recovery y buscamos el servidor de virtualización, al expandir su configuración nos mostrará el inventario de equipos que tiene respaldados, aquí podemos apreciar al servidor asrvm01 que respaldamos anteriormente. De aquí vamos a tener diferentes opciones de puntos de restauración, tanto por fechas como por origen de los datos. Para efectos de la prueba queremos restaurar del sitio secundario, es decir los respaldos desde el Cloud, por lo que buscamos una opción de recover from online.



Al igual que el controlador de dominio en el paso anterior, el servidor web permite únicamente la restauración en un folder compartido. Desde un servidor web recuperamos los componentes que necesitamos o bien remplazamos completo el folder llamado inetpub donde se deposita todo el contenido web.

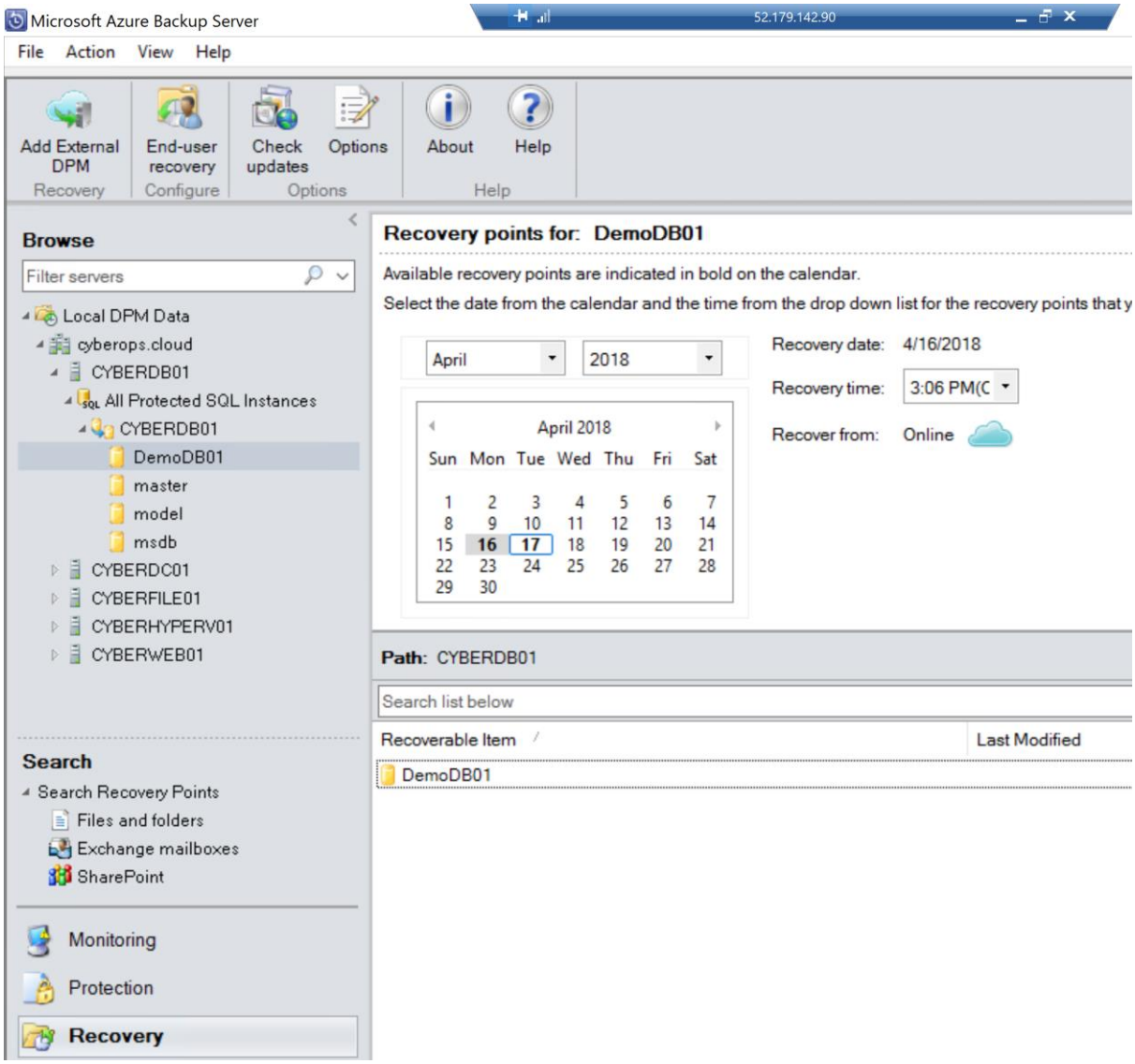


Validación del folder donde se depositaron los datos de respaldo.

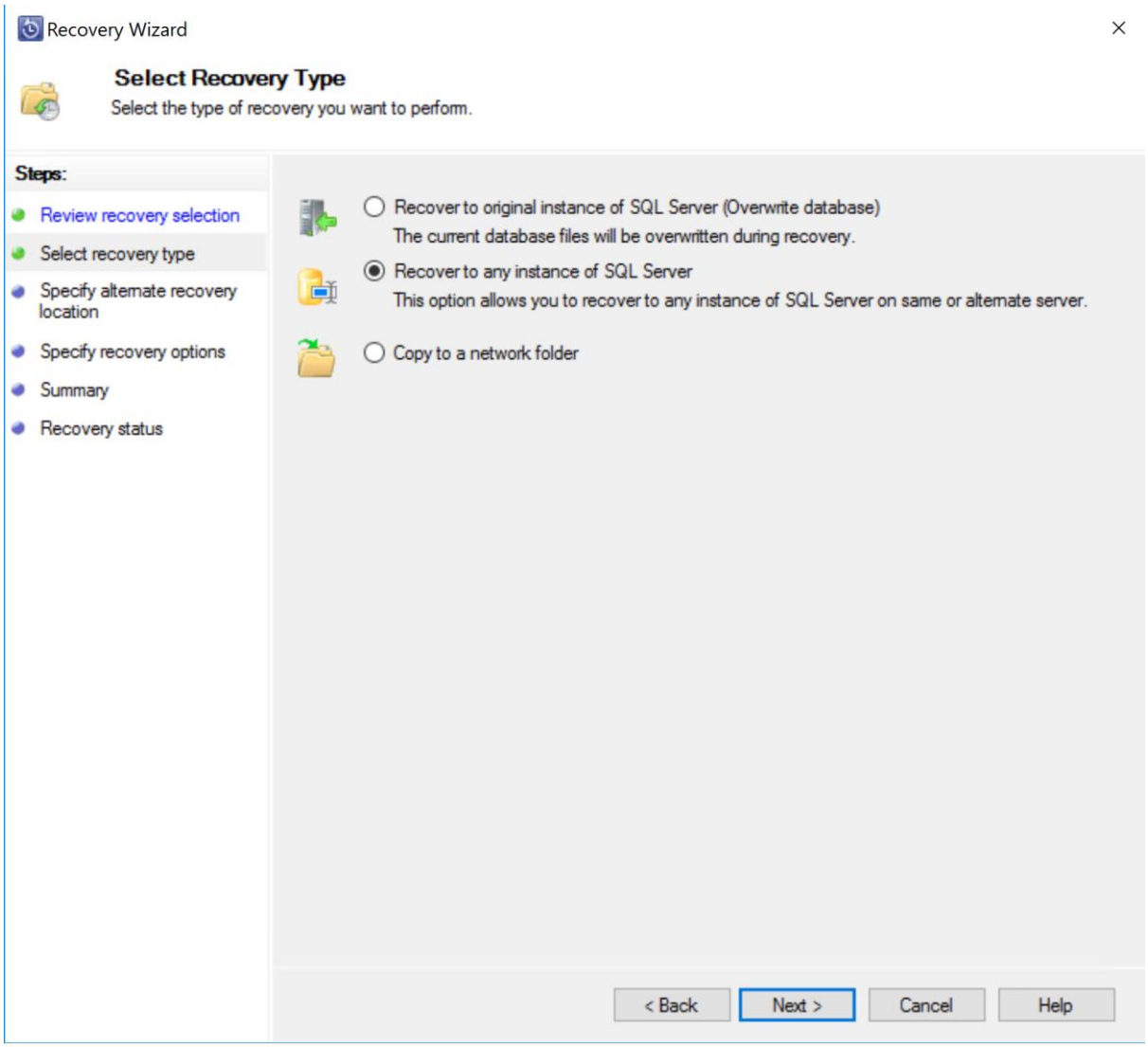


Restauración base de datos

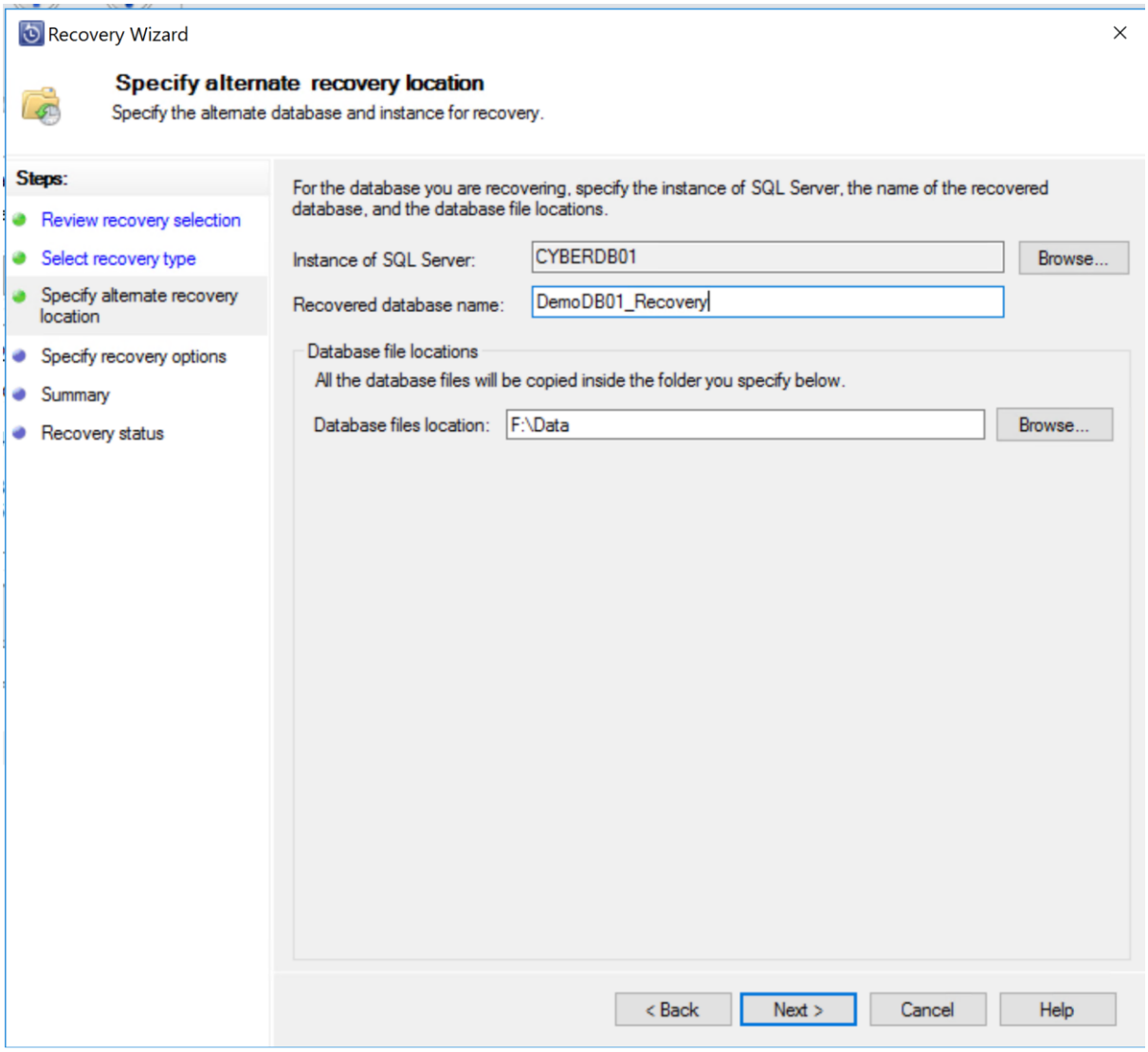
Desde la herramienta de respaldos, navegamos a recovery y buscamos el servidor de virtualización, al expandir su configuración nos mostrará el inventario de equipos que tiene respaldados, aquí podemos apreciar al servidor CyberDB01 y específicamente la base de datos DemoDB01 que respaldamos anteriormente. De aquí vamos a tener diferentes opciones de puntos de restauración, tanto por fechas como por origen de los datos. Para efectos de la prueba queremos restaurar del sitio secundario, es decir los respaldos desde el Cloud, por lo que buscamos una opción de recover from online.



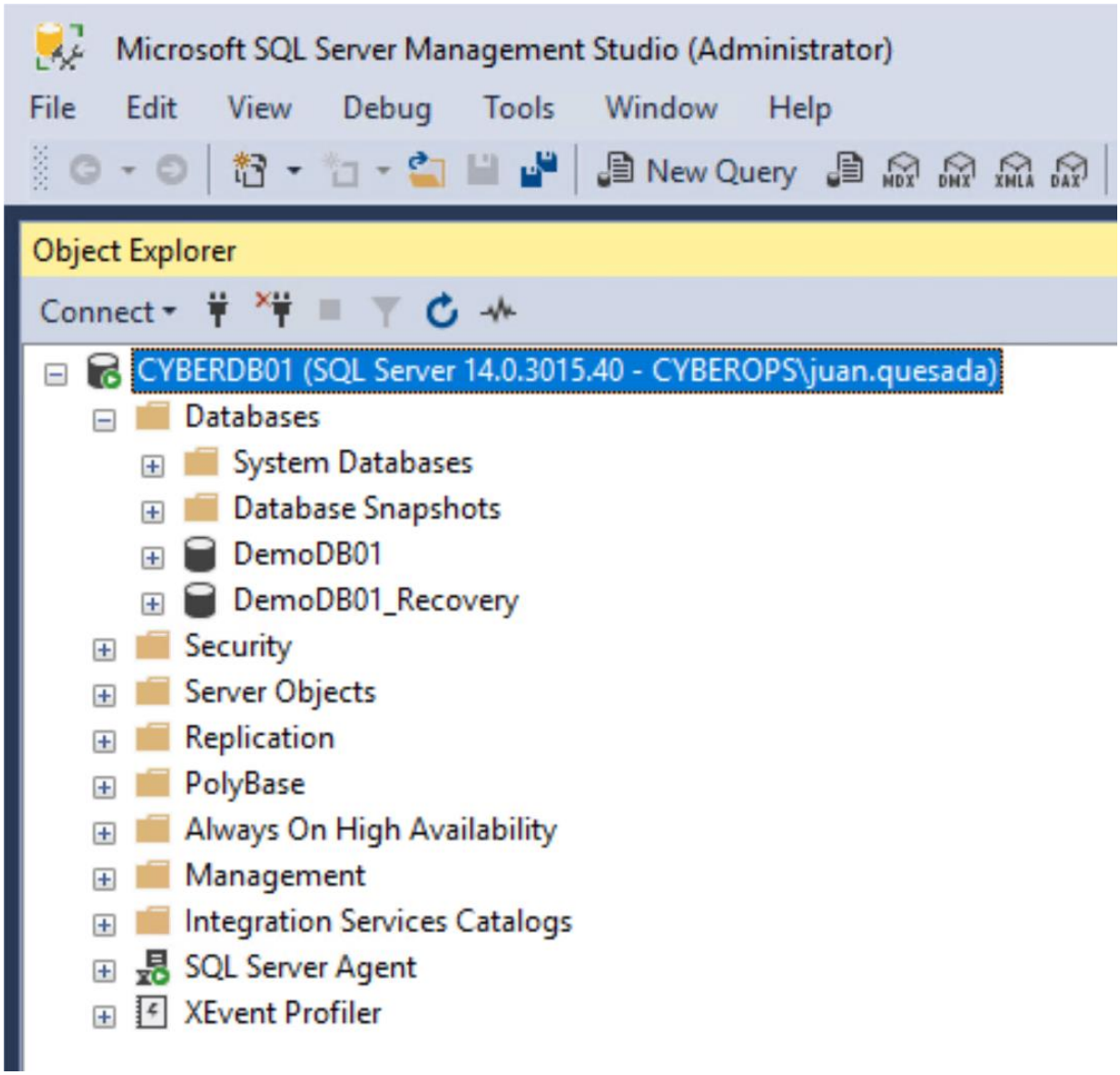
Para una restauración en producción tenemos dos alternativas, restauración completa que sobrescribe la base de datos actual, o restaurar la base de datos con otro nombre para recuperar datos parciales. Para efectos de pruebas mensuales se recomienda restaurarlo sobre un servidor de base de datos no productivos, como mencionamos anteriormente.



Para efectos de esta restauración, renombramos la base de datos a DemoDB01_Recovery.

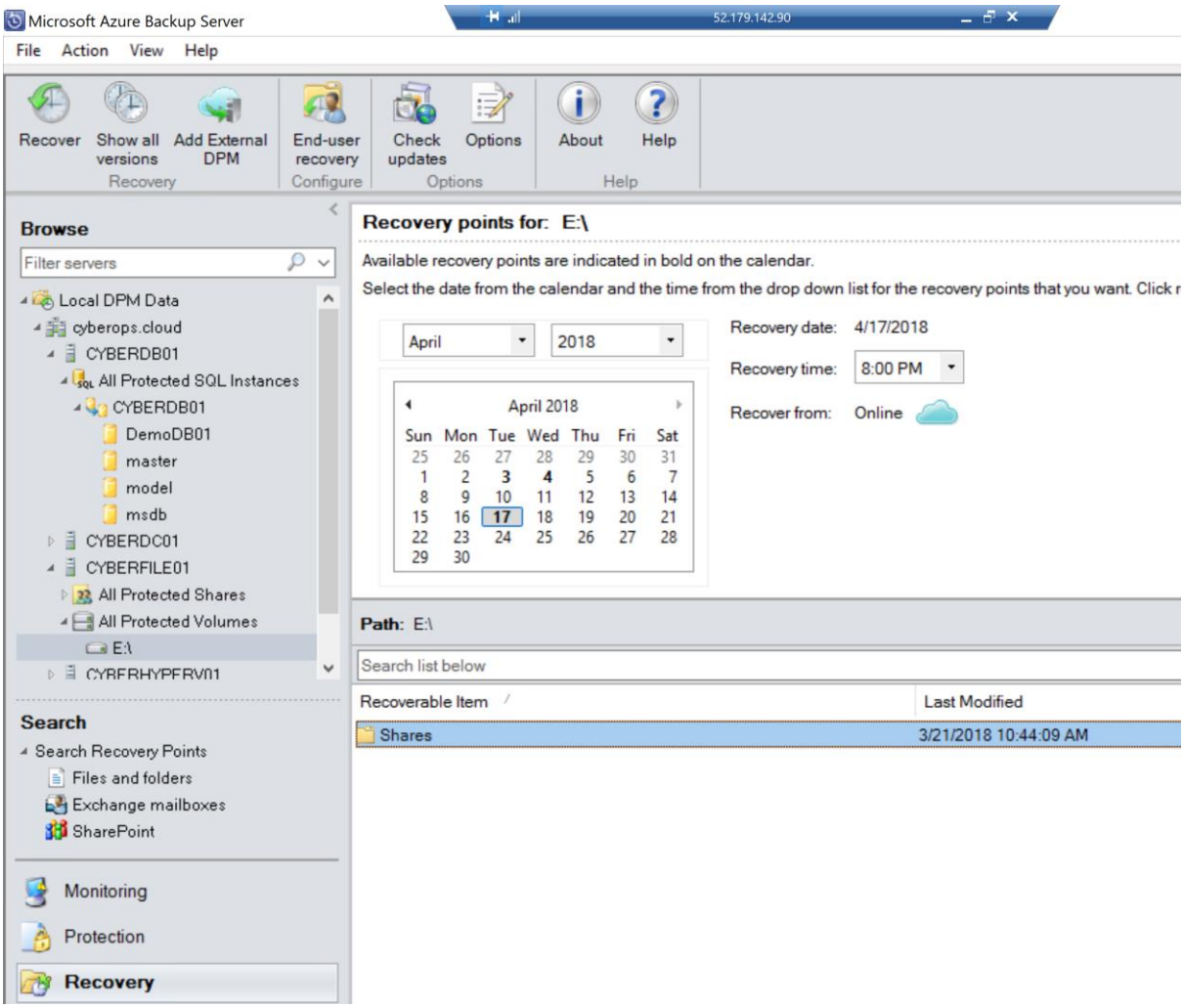


Luego de completada la transferencia de datos podemos validar a nivel de la herramienta de base de datos, la instancia y sus tablas. Posterior a su revisión o restauración, se procede normalmente a eliminar la instancia.

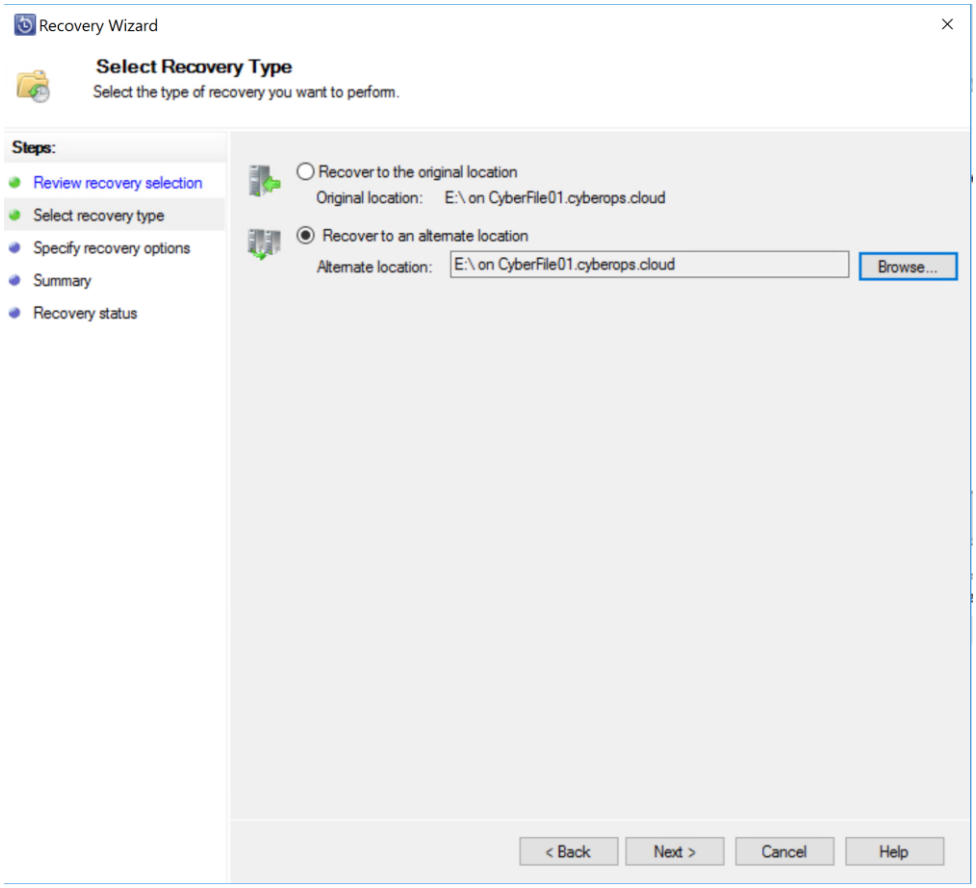


Restauración servidor de archivos

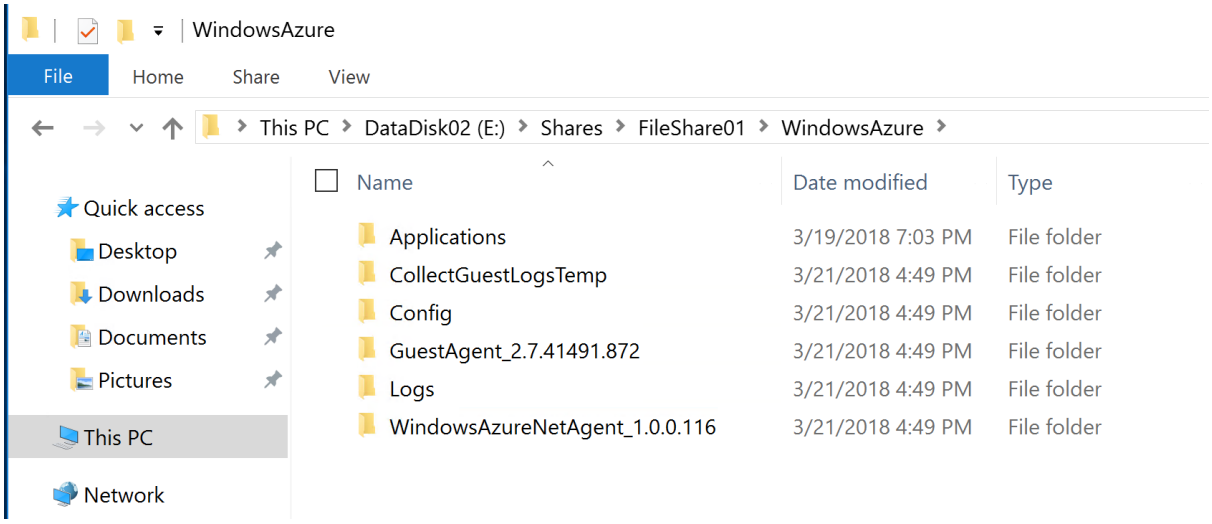
Desde la herramienta de respaldos, navegamos a recovery y buscamos el servidor de virtualización, al expandir su configuración nos mostrará el inventario de equipos que tiene respaldados, aquí podemos apreciar al servidor cyberfile01 que respaldamos anteriormente. De aquí vamos a tener diferentes opciones de puntos de restauración, tanto por fechas como por origen de los datos. Para efectos de la prueba queremos restaurar del sitio secundario, es decir los respaldos desde el Cloud, por lo que buscamos una opción de recover from online.



En caso de una recuperación real podemos restaurar sobre el mismo servidor, el sistema nos da opción de sobrescribir archivos si existen, de crear una segunda copia o bien no sobrescribirlos. De igual modo archivos que no existen los recupera completos. Para efectos de pruebas preferimos restaurar sobre una ruta alterna, así no afectamos el ambiente productivo.

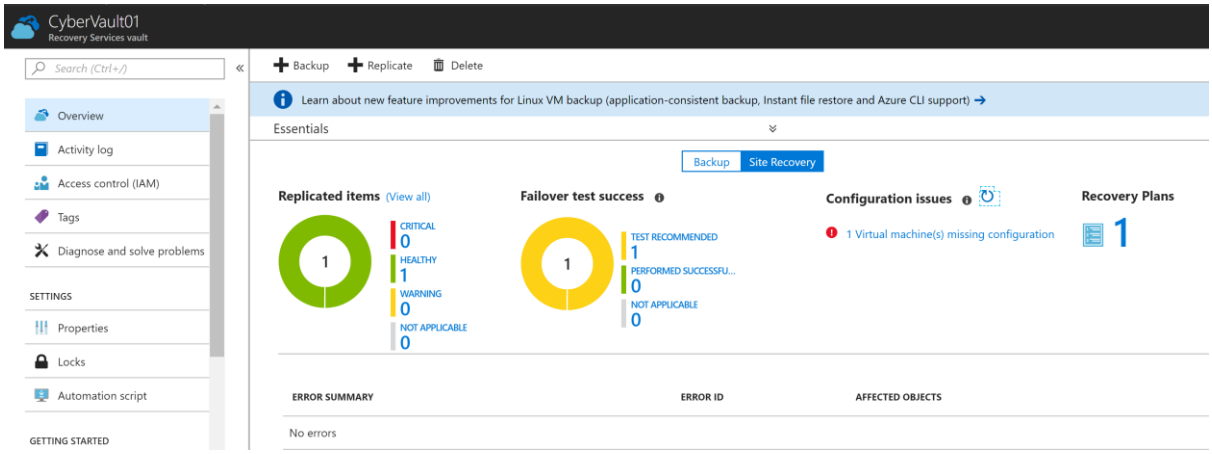


Una vez restaurados los datos podemos validar los mismos y comparar su funcionalidad. Para eliminarlos sencillamente realizamos un borrado normal de archivos.

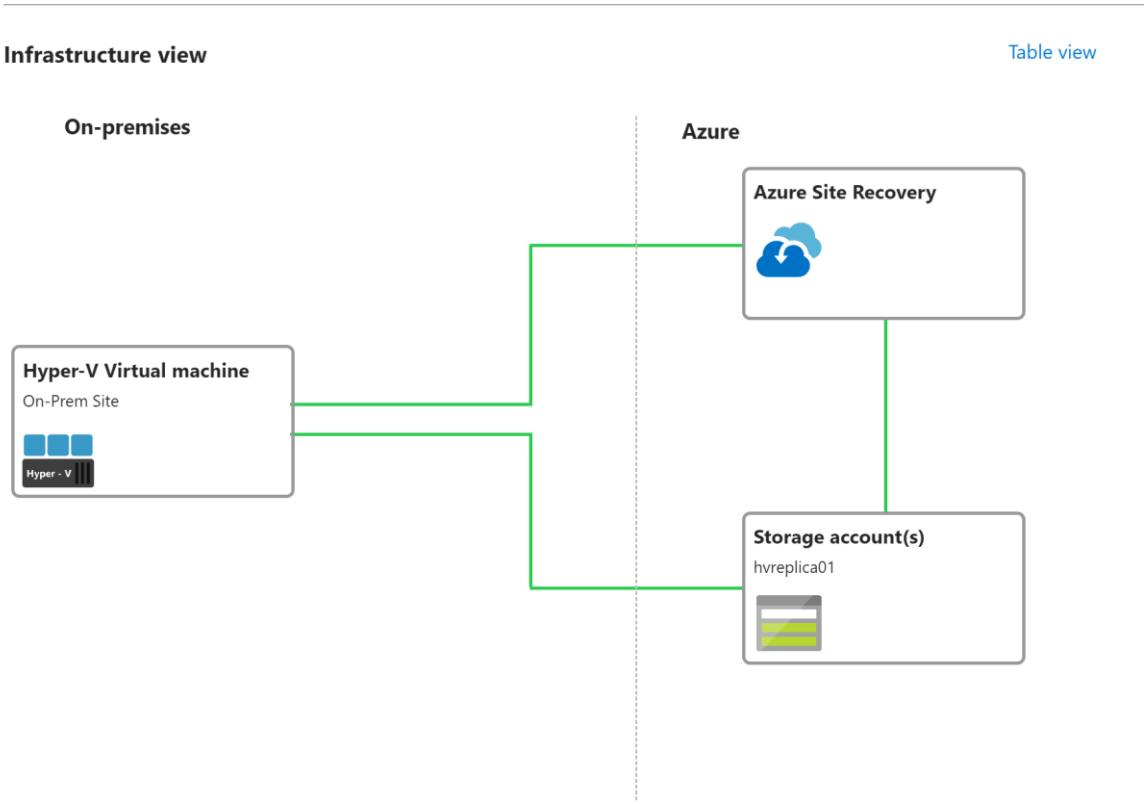


Prueba de réplica de servidor a sitio secundario

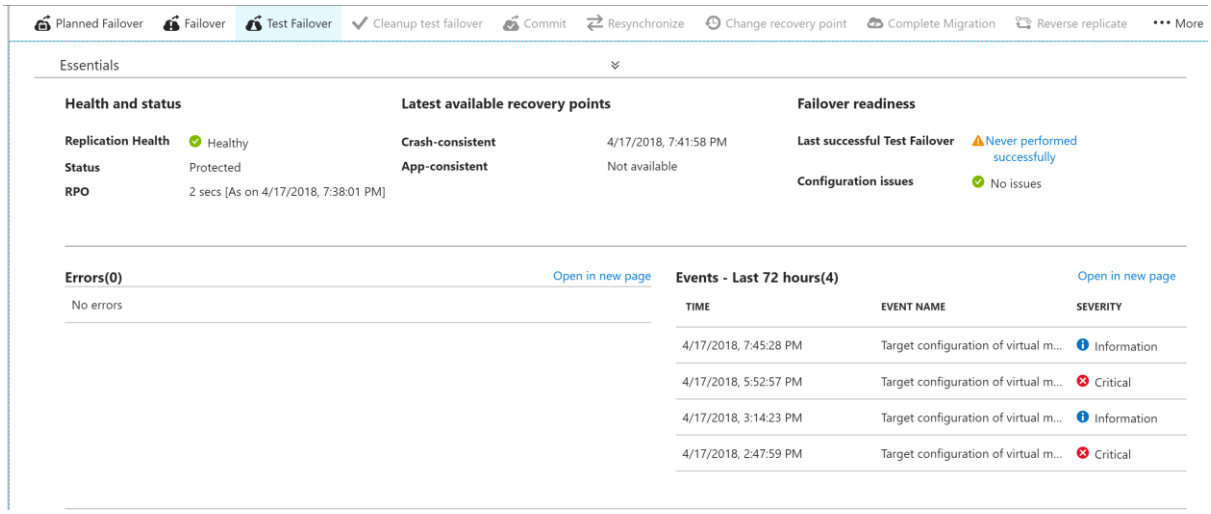
El servidor replicado, a diferencia del respaldo, nos permite levantar los servidores en un segundo sitio y continuar operativa desde aquí en caso de que el sitio principal se encuentre comprometido por una falla, un desastre natural, o un ataque humano. Esto entre las varias opciones que mencionamos en capítulos iniciales. Dado que en este escenario el sitio principal no está disponible, iniciamos el proceso directo desde el sitio secundario, es decir, desde la nube de Azure. Para esto navegamos al ya conocido portal, abrimos la bóveda y seleccionamos la opción site recovery.



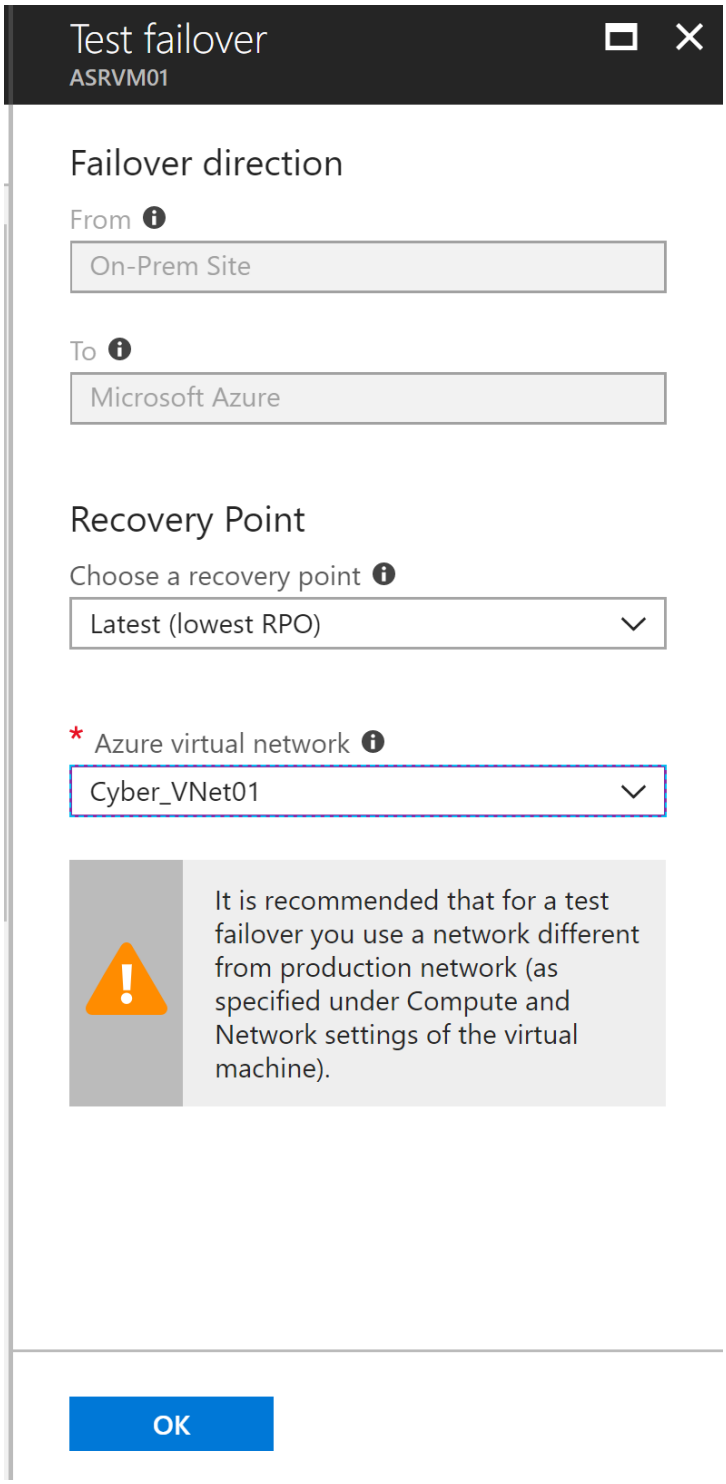
Esto nos muestra nuestro escenario, un servidor Hyper-v en sitio replicado contra el almacenamiento en la nube mediante el orquestador de la nube.



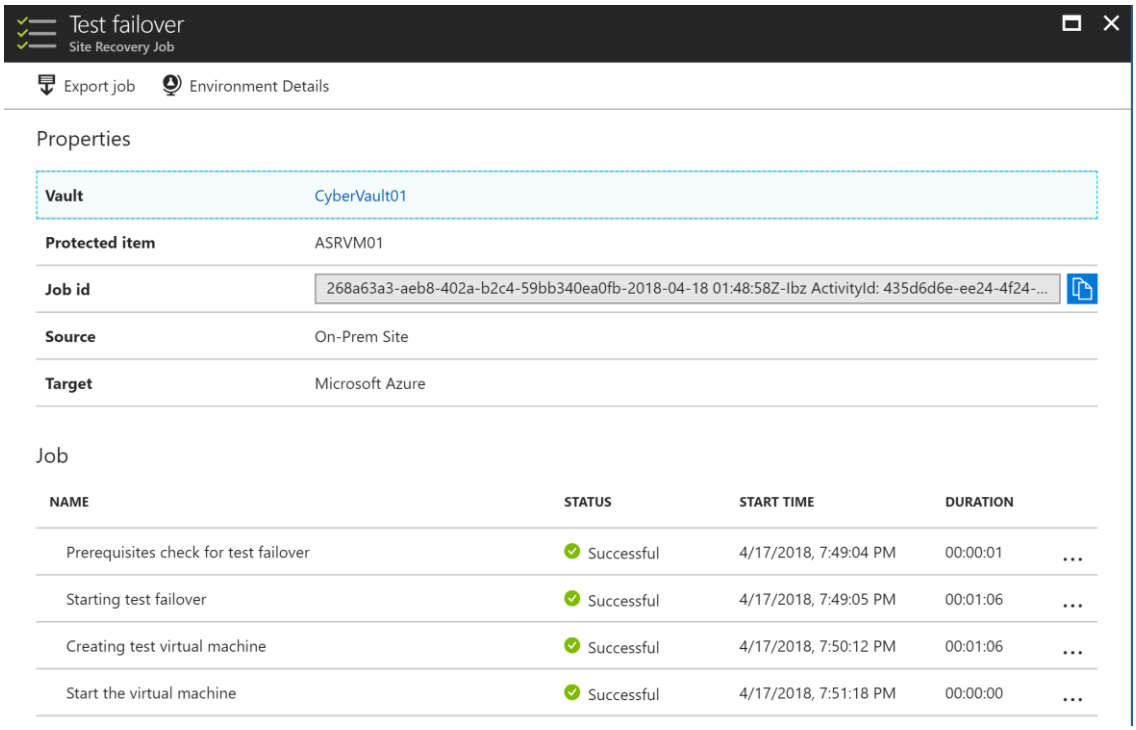
Seleccionamos el servidor que queremos probar, en este caso la máquina virtual asrvm01 que configuramos anteriormente. Aquí como se aprecia tenemos una opción dedicada para pruebas que se llama test failover o prueba de falla. Vamos a continuar con la misma haciendo una aclaración importante, la opción test failover si bien sigue el mismo proceso de un failover real y su opción que se muestra en pantalla, la misma difiere en que esta primera no afecta el ambiente primario. Es decir, un failover migra al sitio secundario y apaga el sitio primario en caso de que esté accesible, mientras que un test failover crea un ambiente secundario sin afectar el primario, opción sumamente valiosa para pruebas.



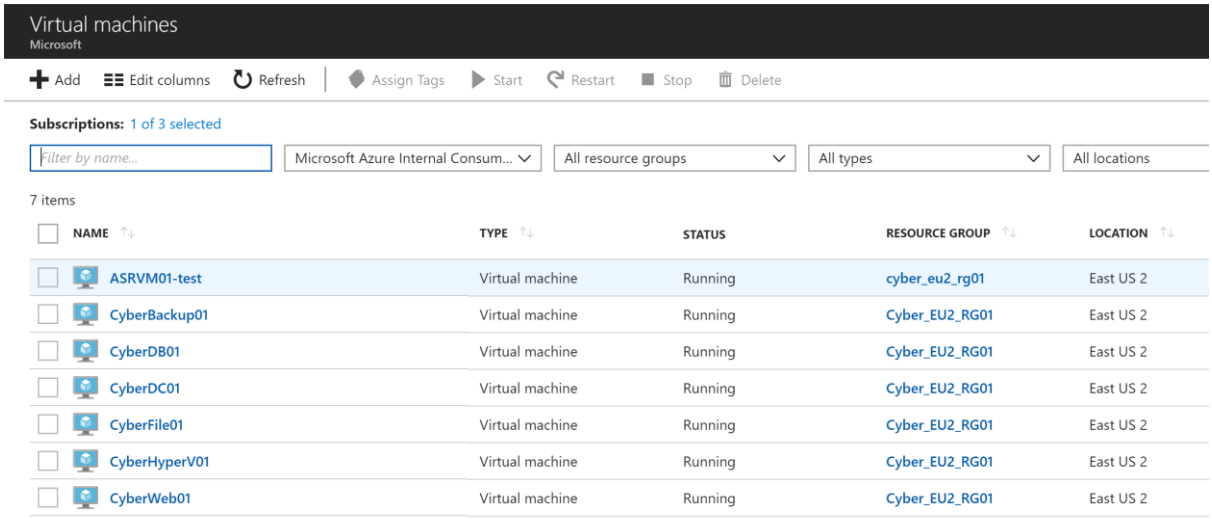
El sistema nos pide seleccionar qué versión queremos restaurar, recordemos que en la configuración nos pedía cuántos puntos de restauración queremos, aquí el sistema nos permite escogerlos, así como en cuál red queremos que el servidor esté.



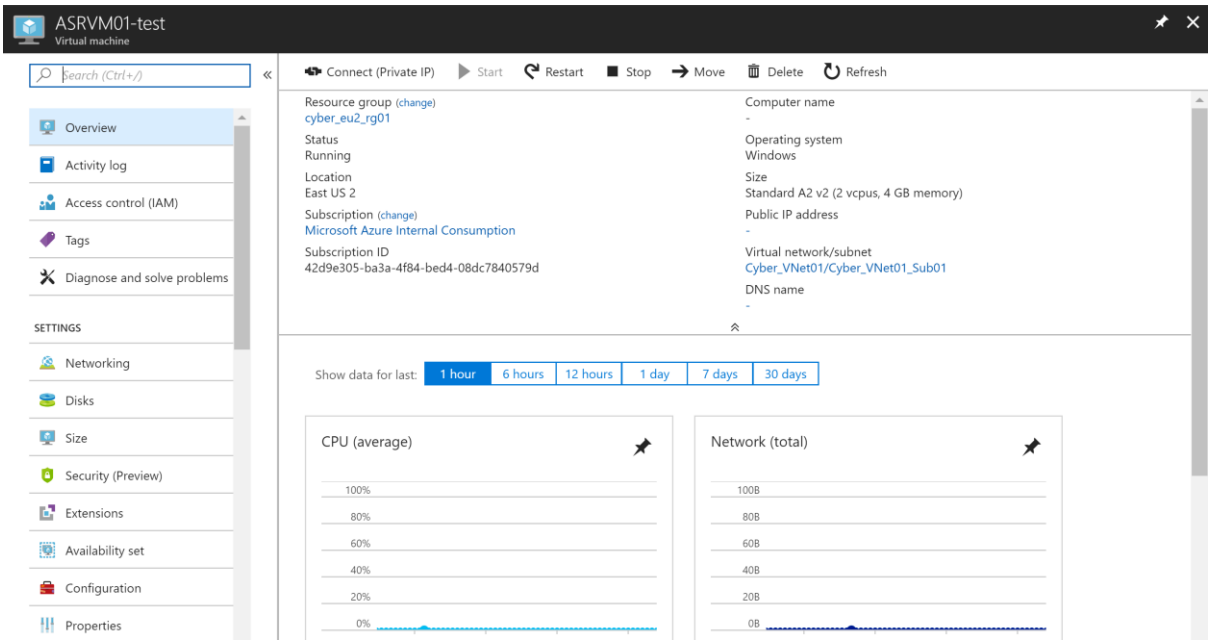
Esperamos un tiempo, normalmente de pocos minutos, como se puede apreciar en la imagen, para que el servidor secundario esté encendido y operacional. Es asombroso lo rápido que esta tecnología trabaja.



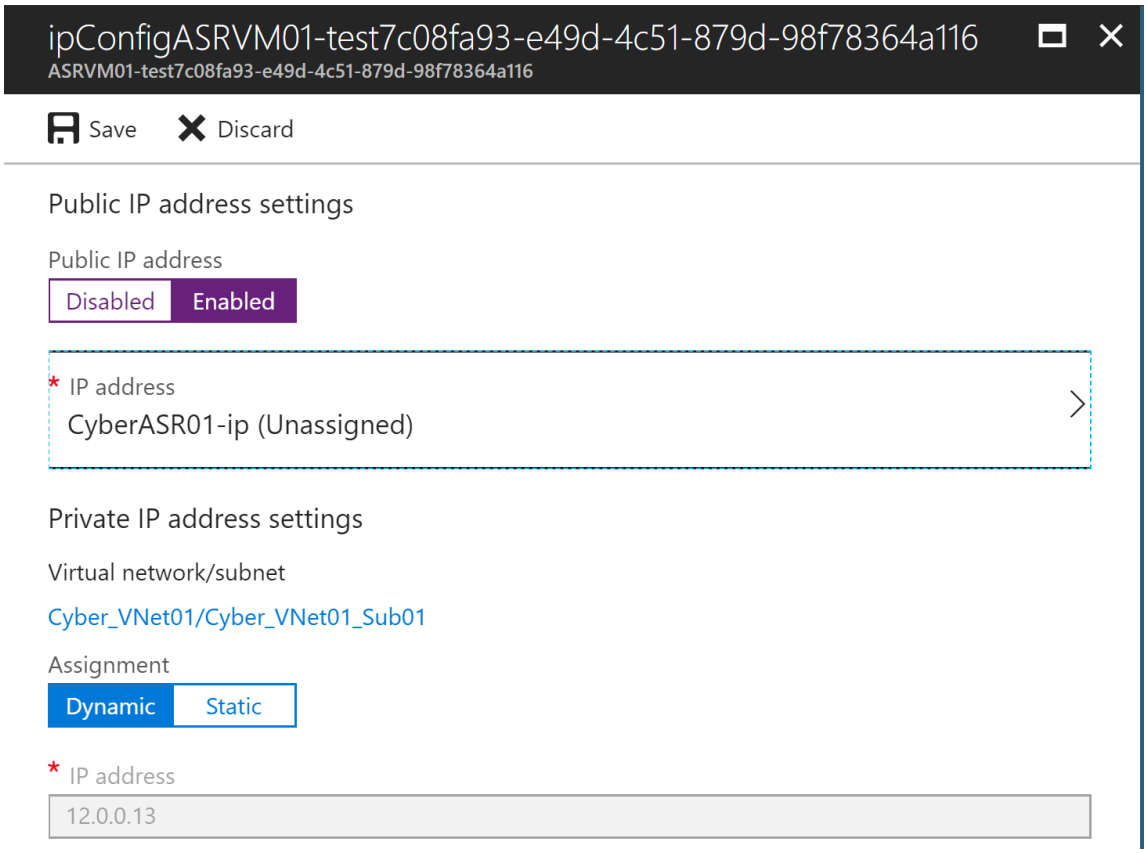
Luego de recuperado, podemos apreciar en la nube de Azure los servidores operando, aquí se puede observar cómo queda operativo el servidor ASRVM01-test.



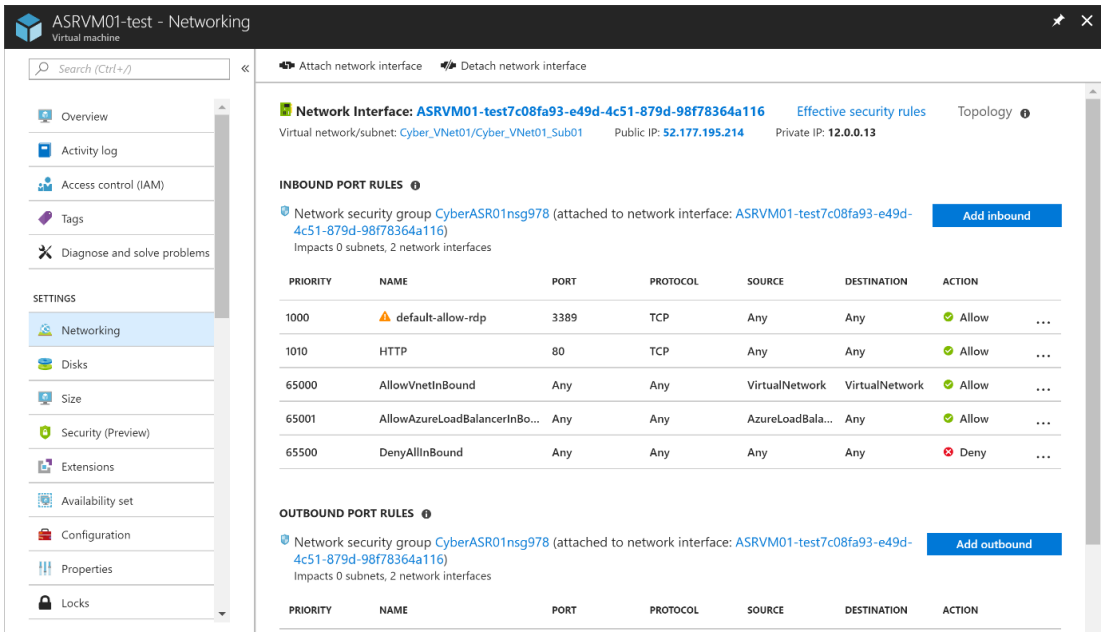
Entramos a la configuración del servidor y vemos que ya está operando, para efectos de la recuperación el mismo no puede ser accedido por una IP Pública, pero le asignaremos una para poder ingresar al equipo y validar su operación.



Para esto entramos a la configuración de red del servidor y le asignamos una IP Pública, es tan fácil como un clic que miramos en la imagen.

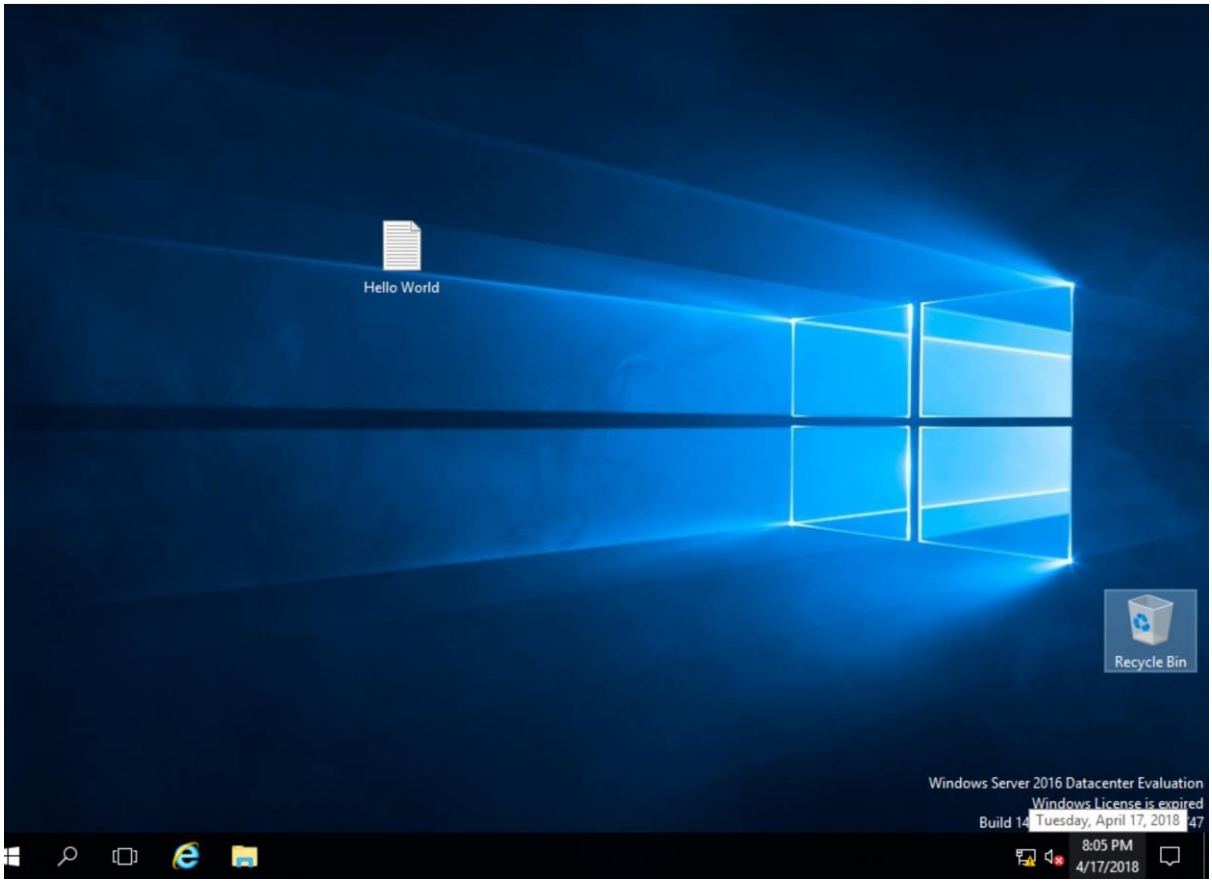


El segundo paso es iniciar con los contrafuegos que permitan el acceso al puedo de escritorio remoto. Este es el puerto 3389, como se muestra en la imagen.

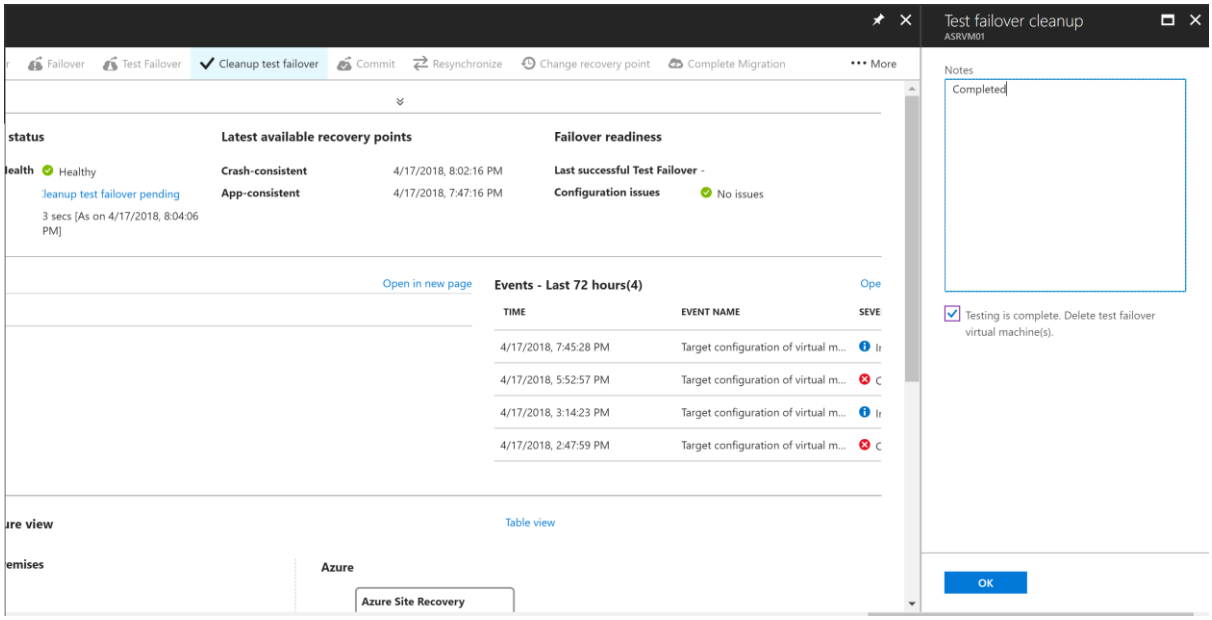


Por ultimo, se requiere dar clic en conectar al servidor del cual descarga un archivo RDP con la configuración, damos doble cllic al mismo e ingresamos las credenciales del servidor. Así de sencillo y ya tenemos acceso al servidor en el sitio secundario.

Es necesario aclarar que para un escenario real existen varias alternativas para conectarse al centro secundario, ya sea que publiquemos los servicios por una IP Pública o bien establecer una conexión VPN. La necesidad real depende del esquema que la empresa quiera tomar.



Ya por terminada la prueba, volvemos al portal de Azure y en la bóveda tendremos una opción de limpiar la prueba. En un clic el sistema se encarga de destruir la máquina virtual secundaria y reiniciar la réplica de datos normal.



Las pruebas de restauración son sencillas y permiten realizarse constantemente para verificación sin invertir mucho tiempo o recursos en las mismas. Un precio bajo para asegurar que nuestros sistemas de recuperación implementados realmente funcionan y estamos protegiendo a la empresa.

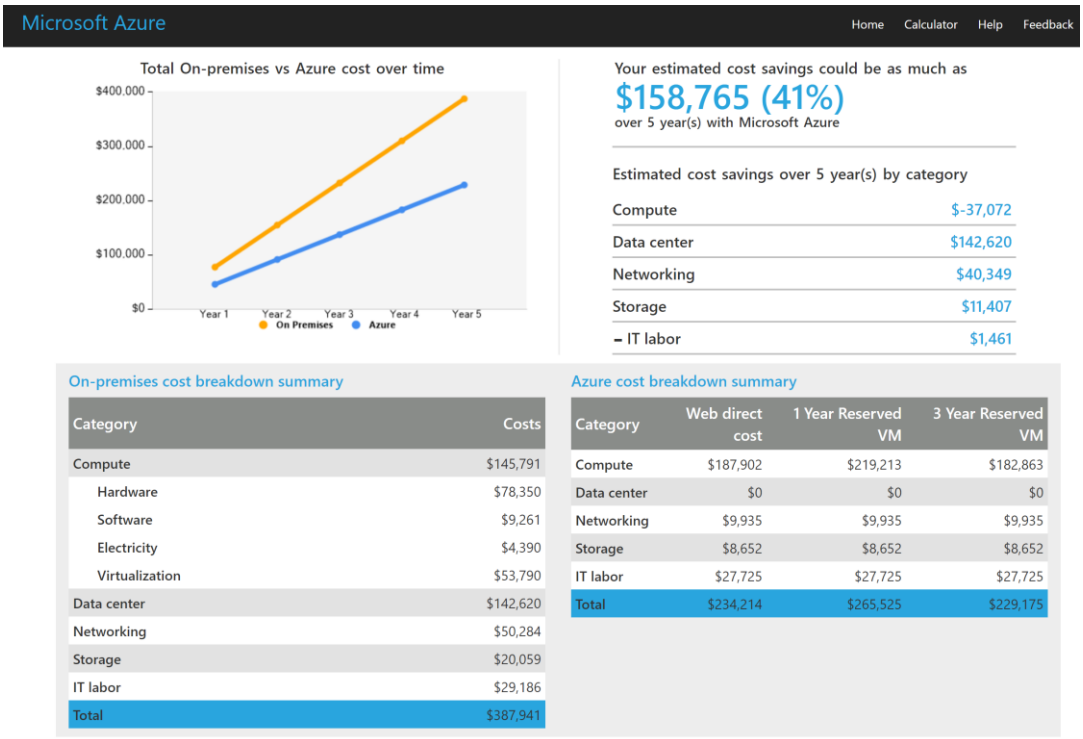
Cloud como sitio Primario para pymes

En la información presentada en este documento podemos apreciar cómo la computación en la nube es innovadora, flexible y costo-efectiva para casos de recuperación contra desastres. Su innovación es mucho mayor cuando usamos los múltiples servicios adicionales que tiene de cómputo, bases de datos como servicios, páginas web como servicios, servicios de analítica e inteligencia artificial que nos permiten hacer predicciones de negocio avanzadas, entre muchos de los servicios.

De esta manera, es claro que las empresas si ya tienen inversiones en centros de cómputo y equipo local, esta inversión no debe ser despreciada, pero, como es tendencia mundial, se recomienda ir mirando la nube como sitio principal. Esto permite a la pyme deshacerse del costo capital de equipos, contratos de soporte, personal capacitado, sobre o subdimensionamiento de recursos que generan pérdidas o bien falta de agilidad.

El sitio web www.tco.microsoft.com provee una calculadora que compara los costos de comprar, operar y mantener un centro de datos local vs utilización de Azure. Esta calculadora es certificada por un tercero llamado Nucleus research basado en análisis financieros reales.

Para dar un ejemplo, usamos la calculadora seleccionando 15 servidores virtuales corriendo sobre plataforma de virtualización hyper-v, con 4 CPU y 8GB promedio en memoria RAM con 2TB de almacenamiento en disco y 8TB para respaldo. El resultado nos indica que la nube representa hasta un 41% de ahorros en 5 años (3 años es la garantía normal de un equipo más dos años de garantía extendida, ya a partir del 5to año no se recomienda seguir utilizando el equipo por obsolescencia tecnológica).



Poder ahorrar 150mil dólares en 5 años para una Pyme representa un ahorro considerable, más aún cuando la computación en la nube permite pagos mensuales y no un monto alto por adelantado, lo que ayuda así al flujo de caja de la empresa. Esto además asegura que no hay subutilización de equipos, menor preocupación de carga operativa, mayor agilidad de crecimiento e innovación de productos y permite esquemas de recuperación contra desastres aún más fáciles, considerando que por standard la mayoría de los servicios Cloud ya incluyen un nivel de disponibilidad mayor a 99%.

Para agregar valor, todo este esquema de recuperación contra desastres es muchas veces utilizado como un primer paso para completar una migración hacia la nube, es decir, si nuestro sitio secundario queda sin capacidad, ocurre un desastre irrecuperable o bien obsolescencia tecnológica, lo que hemos hecho anteriormente nos permite migrar a la nube y continuar la operación allá. De igual manera la nube permite esquemas de recuperación contra desastres que son similares e incluso más sencillos de implementar que lo que hemos visto aquí. Esto permite que este esquema de desastres no solamente dé valor al permitir la continuidad de negocio, sino que nos pone un paso sobre una modernización de centro de datos en la nube.

Conclusiones

- Una continuidad de negocio apropiada permite a las pymes operar en caso de desastres, ataques o errores humanos.

- La computación en la nube permite un esquema costo-efectivo, simple y flexible para contingencia de datos.

- La implementación y pruebas de los sistemas de contingencia es sencilla y efectiva.

- La recuperación contra desastres en la nube es un primer paso a una migración completa que traerá mayores beneficios a largo plazo.

Recomendaciones

- A pesar de que la tecnología en la nube es sencilla de utilizar, siempre se recomienda contar con un socio experto con capacidad comprobada que asesore e implemente. Si no se tiene el personal capaz para operar post implementación, se recomienda un socio de servicios administrados los cuales se encargarán de monitorear, ajustar y ejecutar una recuperación contra desastres de ser necesario.
- Siempre se debe hacer pruebas, desde la primer post implementación, así como pruebas constantes de los sistemas, estas le ayudarán a tener tranquilidad de que la tecnología funciona además de que mantiene al personal actualizado en el proceso de pruebas y permite identificar ajustes y mejoras en los esquemas.
- Mantener un centro de datos es costoso, mucho más si se incorporan mecanismos para alta disponibilidad en todos los sistemas. La computación en la nube permite inicialmente darles contingencia a los sistemas, pero se puede convertir en el centro de datos primario. Los proveedores de computación en la nube son expertos en las áreas de disponibilidad de servicios y ofrecen niveles de servicio mayores al 99.9% anual, se reduce así la posible incidencia de recuperación contra desastres. De igual manera estos proveedores de servicio tienen tecnologías nativas de respaldo y replicación a un segundo sitio, lo cual simplifica la integración y operación.

Reflexiones Finales

Es realmente apasionante, como tecnólogo, poder trabajar con tecnologías de nube para resolver necesidades de negocio como la continuidad operativa. Estamos en una nueva era de tecnologías extremadamente poderosas e inteligentes al acceso de un computador, tecnologías capaces de permitir a miles y miles de empresas trabajar diariamente a nivel mundial. Operar un centro de datos, cambiar piezas de cómputo, entre otras tareas rutinarias, es sencillamente del pasado. La computación en la nube es un gran lego donde escogemos las piezas que tengan sentido para construir la operativa de una empresa, y sobre todo donde la mayor innovación se está dando.

Finalmente, la llamada transformación digital permite a los empleados mejor colaboración, permite interactuar mejor con nuestros clientes, permite optimizar costos operativos y permite innovar nuestros productos. La recuperación contra desastres en la nube es sencillamente un paso intermedio, híbrido, que permite conectar el mundo tradicional robusteciéndolo mientras damos un paso hacia las nuevas generaciones tecnológicas.

Bibliografía

Danilo José, Mannella Lemos (2012). Diseño de una guía para la implementación del uso de computación en la nube como mecanismo de recuperación ante desastres tecnológicos en PYMES en el DMQ. Maestría en Gerencia de Sistemas. Recuperado el 15 octubre de 2017 de http://repositorio.espe.edu.ec/handle/21000/6252

DisasterRecovery.org (2016) Benefits of Disaster Recovery Using Cloud Computing. Recuperado el 12 noviembre de 2017 de http://www.disasterrecovery.org/benefits-of-disaster-recovery-using-cloud-computing.html

Forrester Research and the Disaster Recovery Journal (2015). The State of Business Continuity Preparedness. Recuperado el 18 octubre de 2017 de http://drj.com/images/surveys_pdf/forrester/2014-Forrester-Survey.pdf

Forrester Research and the Disaster Recovery Journal (2014). The State of IT Resiliency and Preparedness. Recuperado el 18 octubre de 2017 de https://www.drj.com/images/surveys_pdf/forrester/2013-Forrester-Survey.pdf

Forrester Research, Inc (2014) The State of Business Technology Resiliency, Q2 2014. Recuperado el 12 noviembre de 2017 de https://www.techrepublic.com/resource-library/whitepapers/forrester-paper-the-state-of-business-technology-resiliency-q2-2014/

Gartner (2010) What is SMB? - Gartner Defines Small and Midsize Businesses recuperado el 28 de setiembre de https://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses

IDC (2011) Best Practices in Business Continuity and Disaster Recovery. Recuperado el 12 noviembre de 2017 de https://www.riverbed.com/document/fpo/media-cms/Whitepaper-Riverbed-IDC-Best-Practices-DR.pdf

IDC en colaboración con AppDynamics de Cisco (2015) DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified recuperado el 17 setiembre de 2017 de http://devopsdigest.com/idc-survey-appdynamics-devops-application-performance

Microsoft (2017) Institución hospitalaria obtiene alta disponibilidad y ahorro de costos al migrar a la nube recuperado el 13 marzo de https://customers.microsoft.com/en-us/story/hospital-cima-azure-cloud-services-office365-health-costa-rica

Microsoft (2018) Site Recovery Documentation recuperado el 13 marzo de https://docs.microsoft.com/en-us/azure/site-recovery/

Microsoft (2018) Azure Backup Documentation recuperado el 13 marzo de https://docs.microsoft.com/en-us/azure/backup/

Symantec (2011) Symantec 2011 SMB Disaster Preparedness Survey. Recuperado el 9 noviembre de 2017 de http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf

Wall Street Journal (2017) Amazon Finds the Cause of Its AWS Outage: A Typo. recuperado el 19 marzo 2018 de https://www.wsj.com/articles/amazon-finds-the-cause-of-its-aws-outage-a-typo-1488490506