Universidad católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

"TRANSICIÓN DE APLICACIONES A LA NUBE BAJO TECNOLOGÍAS DISEÑADAS EN ALTA DISPONIBILIDAD"

Tesis Presentada por la Bachiller:
Zevallos Rivera, Claudia Milagros

Para optar el Título Profesional de:
Ingeniera de Sistemas con especialidad en Ingeniería de Software

Asesor:
Ing. Fernández del Carpio, Álvaro

AREQUIPA - PERÚ
2017

PRESENTACIÓN

Sr. Director de la Escuela Profesional de Ingeniería de Sistemas.

Sres. Miembros del Jurado.

De conformidad con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas, pongo a vuestra consideración el presente trabajo de investigación titulado: “TRANSICIÓN DE APLICACIONES A LA NUBE BAJO TECNOLOGÍAS DISEÑADAS EN ALTA DISPONIBILIDAD”, el mismo que de ser aprobado me permitirá optar el Título Profesional de Ingeniería de Sistemas.

Claudia Milagros Zevallos Rivera

RESÚMEN

Los sistemas de computación en la nube o cloud computing actualmente están abasteciendo a las diferentes compañías a nivel mundial.

La adopción de esta tecnología en los departamentos de TI para sus diferentes servicios representa seguridad, disponibilidad y prevención ante fallos, facilidad de escalamiento de software frente a un aumento de solicitudes hacia los servicios publicados, reducción en el tiempo de ejecución y bajo costo, ya que el pago es por uso.

Las soluciones y creación de infraestructura en la nube son caracterizadas y adecuadas a la situación en la que se encuentra la empresa, a sus necesidades y requerimientos para la optimización de sus procesos e incremento tecnológico.

Los datos generados por los servicios publicados y la correcta gestión de ellos con las herramientas adecuadas impactan de manera positiva en el proceso de toma de decisiones de las empresas, lo cual se ve reflejado en la optimización de tiempos y reducción de costos.

En este proyecto se presenta la transición y alojamiento en la nube de las aplicaciones web de una institución pública, incluyendo el portal institucional y servicios de integración. La capacidad de cómputo implementada sirve para garantizar la disponibilidad de recursos en el cloud hosting de la institución pública que permite afrontar las necesidades de cómputo.

Palabras Claves: (Alojamiento, IaaS, Nube, Web, Disponibilidad, Almacenamiento).

ABSTRACT

The computer systems in the cloud or cloud computing are currently supplying to different companies around the world.

The adoption of this technology in IT departments for their different services represents security, availability and prevention, ease of scaling software compared to an increase of requests to the published services, reduction in execution time and low cost since the payment is for use.

The solutions and creation of infrastructure in the cloud are characterized and appropriate to the situation in which the company is located, to their needs and requirements for the optimization of technological processes and increase.

The data generated by the services that are published and the proper management of them with the proper tools impact positively in the decision-making process of the companies, which is reflected in the optimization of time and costs.

In this project presents the transition and cloud hosting of web applications of a public institution, including the institutional portal and integration services. The computing capacity implemented serves to ensure the availability of resources in the cloud hosting of the public institution that enables you to meet the needs of computation.

Keywords: (Hosting, IaaS, Cloud, Web, Disponibility, Storage).

INTRODUCCIÓN

El avance de la tecnología y la adopción de la misma por grandes y pequeñas compañías hacen del cloud computing un requerimiento estratégico en las oficinas de TI que está enfocado en una inversión para la optimización de sus servicios. El crecimiento en la transición de servicios a la nube se ha incrementado en un 50% por año a la estimación que se tenía para una escala de tiempo de 10 años. Las aplicaciones que son cruciales en dichas empresas y están publicadas en Internet tienen que estar siempre disponibles y sobre todo protegidas. (Microsoft, 2016).

En el presente trabajo se diseñó la arquitectura en alta disponibilidad para la migración a la nube del servicio portal web y aplicativos integrados del Senace, se implementó el escenario diseñado junto a todos sus componentes en la plataforma Microsoft Azure con el modelo infraestructura como servicio, teniendo en cuenta el balanceo de carga de los servidores y la alta disponibilidad, acreditando que la solución cuenta con centros de datos redundantes a nivel mundial. Con la implementación en la plataforma de Azure se tiene la capacidad de realizar escalamientos hacia el fabricante de la solución implementada de cloud computing con el propósito de solucionar cualquier incidente del servicio propuesto.

En la siguiente implementación se genera un gran volumen de data proveniente de las solicitudes a los servicios publicados, la cual es transformada en información relevante para la organización, presentada en un ambiente gráfico, Power Bi, es la herramienta enfocada al análisis empresarial que ayuda a la toma de decisiones para la optimización de la infraestructura creada en la nube, prevención de riesgos y control de uso.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Capítulo 1: Descripción del Proyecto

1.1 Objetivos

Objetivo General

Transición de aplicaciones a la nube bajo tecnologías diseñadas en alta disponibilidad.

Objetivos Específicos

1. Agilizar los procesos con servicios de alta disponibilidad y seguridad avanzada de nivel empresarial.
2. Integrar de manera flexible sistemas operativos, lenguajes de programación y diversas plataformas.
3. Prevenir cualquier tipo de ataque que pueda vulnerar la seguridad de la información organizacional.
4. Reducir riesgos operativos e incrementar el uso de tecnología.
5. Favorecer a la correcta toma de decisiones empresariales con el uso de tecnologías de la información.

1.2 Alcances y Limitaciones

1.2.1 Alcance del proyecto

Diseño e implementación del servicio de alojamiento en la nube de las aplicaciones web del SENACE, incluyendo el portal institucional y el servicio de integración con el SEAL del MINEM. La capacidad de cómputo servirá para garantizar la alta disponibilidad de recursos en el cloud hosting de SENACE que permitan afrontar las necesidades de cómputo respecto a las solicitudes de los usuarios, detallando un aproximado de 2000 conexiones concurrentes.

Se contará con una plataforma de entorno gráfico, que sincronice con los componentes de la infraestructura alojada en la nube para que se visualice el uso y el costo de los mismos, que servirá como fuente de análisis para la toma de decisiones de la organización y así optimizar tiempos en los procesos de análisis y decisión.

El diseño de la arquitectura contemplará y permitirá el correcto balanceo de carga de trabajo y distribuir un tipo específico de tráfico proveniente de internet entre los servidores de la solución, considerando que la aplicación soporta un escenario de alta disponibilidad, el cual habrá sido previamente configurado e implementado.

1.2.2 Limitaciones del proyecto

Cualquier área que no se mencione explícitamente en la sección "Alcance del Proyecto", se considerará como exclusiones del mismo.

- Solución de problemas no originados por las tareas del proyecto.
- Implementar funcionalidades adicionales a las mencionadas como parte del alcance del proyecto.
- Instalación y configuración del Antivirus en la plataforma Azure.
- Configuración de routers, switches, storage y otros componentes de hardware.
- Implementar mecanismo de optimización para la transferencia de datos hacia o desde Azure, basado en productos de terceros o compra de software.
- Instalación de productos de terceros.
- Soporte a las estaciones clientes, servidores y/o parches sobre el sistema operativo.
- Implementación de estrategias recuperación ante desastres.

1.3 Fundamentos Teóricos

1.3.1 Antecedentes del proyecto

Al inicio de la década de 1960, los equipos informáticos solo podían ejecutar un programa a la vez puesto que estaban diseñados y construidos solo para un trabajo específico.

Cinco años después se hizo popular el concepto de tiempo compartido para los recursos de un sistema, es decir la ejecución simultánea de las diversas tareas en un solo equipo.

En 1961 John McCarthy en un discurso en el MIT (Massachusetts Institute Technology) pronóstico que las tecnologías de tiempo compartido podrían manejarse en el que el poder de cómputo y aplicaciones específicas se podrían vender como un servicio.

En 1981 IBM lanzó la "Personal Computer" un equipo con potencia destacable y de precio económico para que pueda ser adquirido por una gran cantidad de usuarios, quienes por la tendencia se acostumbrarían a la capacidad de almacenamiento y tiempos menores en sus procesos.

En 1999 Salesforce llega con el concepto de la entrega de aplicaciones empresariales a través de una página web. Desde allí las empresas optan por la adopción de la publicación de sus aplicativos por medio del Internet.

En el año 2002, Amazon Web Services, provee un conjunto de servicios basados en la nube, donde incluye hardware, almacenamiento e incluso inteligencia de negocios a través de su nube pública. Posteriormente, George Gilder se pronunció con la siguiente aportación: "El PC de escritorio está muerto. Bienvenido a la nube de Internet,

donde un número enrome de instalaciones en todo el planeta almacenarán todos los datos que usted podrá usar alguna vez en su vida".

En el 2009, Google y otras empresas comienzan a ofrecer aplicaciones basadas en navegador, ese mismo año Microsoft entra al mercado con el lanzamiento de Azure, ofreciendo capas de servicio cliente, aplicación, plataforma, infraestructura y servidor.

Para referirse a Cloud Computing la literatura contiene diferentes conceptos, entre los cuales se podrían citar:

El Instituto Nacional para la Estandarización y Tecnología de los Estados Unidos de Norte América (NISI) define como:

"Cloud Computing es un modelo que habilita el acceso a un conjunto de servicios computacionales (e.g. Redes, servidores, almacenamiento, aplicaciones y servicios)".

Cisco Systms Inc: "Recursos de TI que se abstraen de la infraestructura latente y se brindan bajo demanda y a escala en un entorno multiusuario".

En los últimos 10 años la tendencia de las empresas por acortar la distancia de interacción con los usuarios ha llevado a buscar soluciones óptimas en la nube para almacenar y soportar sus aplicaciones.

1.3.2 Bases Teóricas del proyecto

1.3.2.1 Tipos de Nubes

1.3.2.1.1 Nubes Públicas

Según Amrhein (2010) es una infraestructura ofrecida al público por un proveedor de servicios a través de APIs (*application pro-gramming interface* en inglés), para gestionar los recursos sin ser vinculado con el cliente final. Esta retribución se

efectúa de manera autónoma y dinámica por los usuarios a través de las APIs y en función de su uso el servicio es monetizado por los proveedores.

Los servicios, aplicaciones y almacenamiento se ponen a disposición de los usuarios a través de Internet, como servicio, generalmente con un modelo de pago establecido.

Ofrece menos margen de personalización para asegurar el rendimiento y seguridad, reduce la complejidad y los plazos de entrega, debido a que la estructura es fija.

Las nubes públicas son consideradas apropiadas para las empresas que necesitan poner un servicio rápidamente en el mercado, empresas sometidas a menos restricciones normativas y aquellas que buscan externalizar parte o todos sus requisitos de TI.

1.3.2.1.2 Nubes Privadas

Hurwitz (2010) define que las nubes privadas son las que prestan un servicio exclusivo a una organización puesto que son entornos altamente virtualizados del centro de datos ubicado dentro del firewall de la empresa.

Infraestructura cloud implantada exclusivamente personalizada para los requerimientos y estado de una empresa, tanto si se gestiona de forma interna como si un proveedor externo se encarga de ello.

Ofrece soluciones de seguridad avanzada, alta disponibilidad y tolerancia a los fallos que no tienen cabida en la nube pública.

1.3.2.1.3 Nubes Hibridas

Wozniak (2010) se refiere a las nubes híbridas como la combinación de servicios que pertenecen al dominio público y uso privativo, este tipo de nube es el resultado del uso común de características de las nubes públicas y privadas.

Su beneficio principal es la escalabilidad ofrecida por una nube pública con independencia en una privada. Normalmente, las empresas ejecutan una aplicación principalmente en la nube privada, pero utilizan la nube pública para enfrentarse a picos de demanda.

1.3.2.2 Ventajas

1.3.2.2.1 Alta Disponibilidad

Se emplea para definir sistemas redundantes, capaces de soportar la caída de alguno de los componentes del sistema a través del balanceo de carga en la nube.

A&T (2009) indica que la industria de TI se basa en características como proveedores robustos, ciclo de vida y soporte definidos, integración de hosting y servicios de red.

Beneficios:

- Capacidad de escalabilidad y alto desempeño frente a necesidades de incremento o reducción de operaciones hacia los servicios de usuarios y clientes.
- Agilidad organizacional con servicios siempre disponibles y seguridad avanzada de nivel empresarial.
- Flexibilidad de integración con sistemas operativos, plataformas y lenguajes de programación.

1.3.2.2.2 Seguridad

Las soluciones de seguridad son diseñadas para proveer un servicio de análisis, prevención y detección de vulnerabilidades. En base a los requerimientos, se diseña un entorno personalizado para proteger la información de la organización e inversión tecnológica. (Mughal, 2013).

Beneficios:

- Estrategias y modelos a medida para la gestión integral de la seguridad de la información de la organización.
- Disposición de políticas y procedimientos estandarizados de seguridad de la información.
- Detección y prevención de vulnerabilidades a través de sistemas de identificación y sistemas de alerta.
- Evidencias de los posibles impactos de negocio y económicos.

1.3.2.2.3 Analítica

Se apoya en la gestión del gran volumen de información que se genera a través de los productos, áreas, servicios, clientes, competidores y proveedores. Traduciendo los datos en información relevante para la institución y así poder hacer más ágil y efectivo el proceso de toma decisiones y la anticipación de tendencias futuras. (Piatetsky-Shapiro, 2010).

Beneficios:

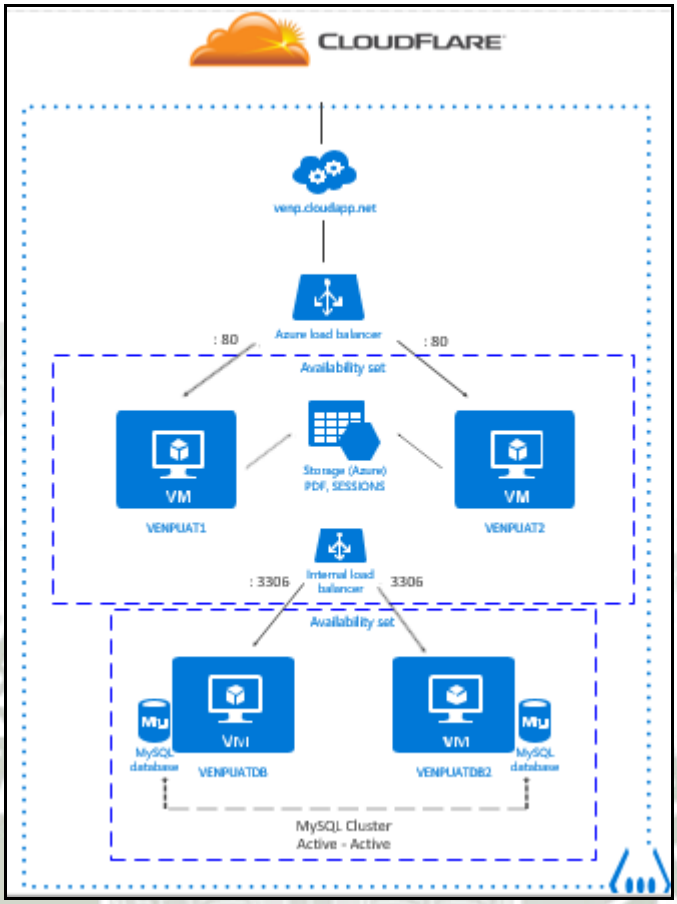
- Disponibilidad de información clave para líderes de áreas de negocios, ventas, operaciones, marketing y TI.
- Mejor conocimiento de comportamientos actuales y potenciales de clientes.
- Medición del impacto y efectividad de iniciativas de negocio.
- Identificación y predicción de nuevas oportunidades de negocio.

1.3.2.3 Tipos de Servicios

1.3.2.3.1 Modelo de Servicio IaaS

Infraestructura como servicio (IaaS) (Figura 1), proporciona recursos de memoria, almacenamiento, CPU, empleando la virtualización, brindando como beneficio la disponibilidad de cualquier servicio puesto permite escalar o reducir los recursos utilizados para ajustarlos a la demanda que se generada por los usuarios. (Washam, 2016).

Figura 1: Arquitectura del servicio IaaS

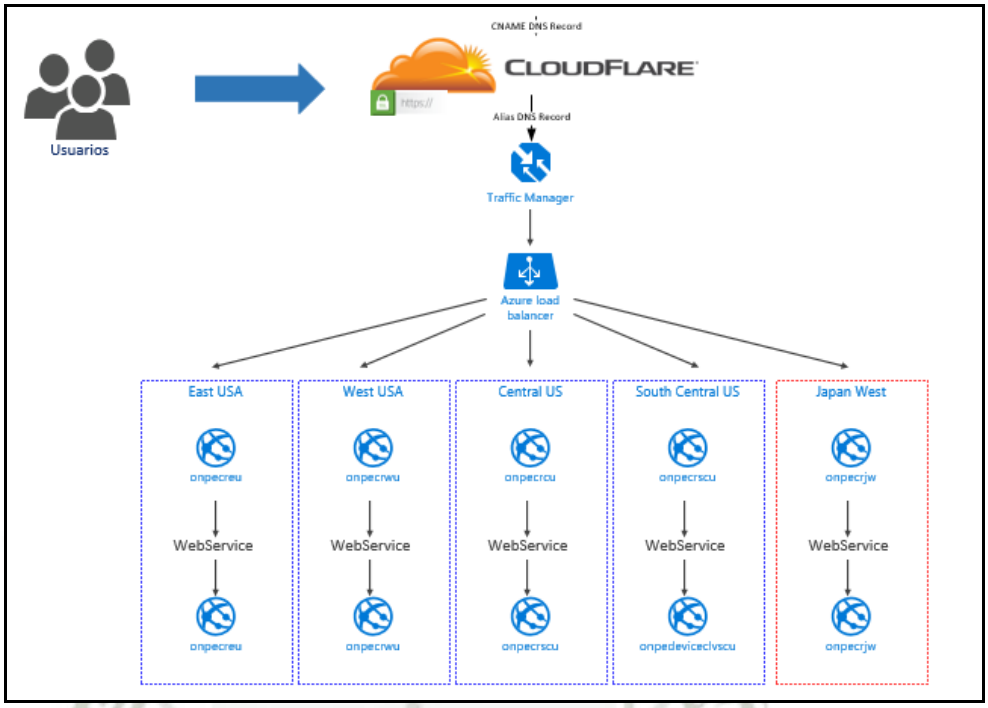


Fuente: Elaboración Propia

1.3.2.3.2 Modelo de Servicio PaaS

Plataforma como Servicio (PaaS) (Figura 2), es un entorno de implementación y desarrollo en la nube que proporciona servidores, almacenamiento y redes del mismo modo que IaaS, pero también incluye herramientas de desarrollo, servicios de inteligencia empresarial para la toma de decisiones y administración de base de datos brindando como beneficio el ciclo de vida completo de las aplicaciones web. (Pietschmann, 2016).

Figura 2: Arquitectura del servicio PaaS

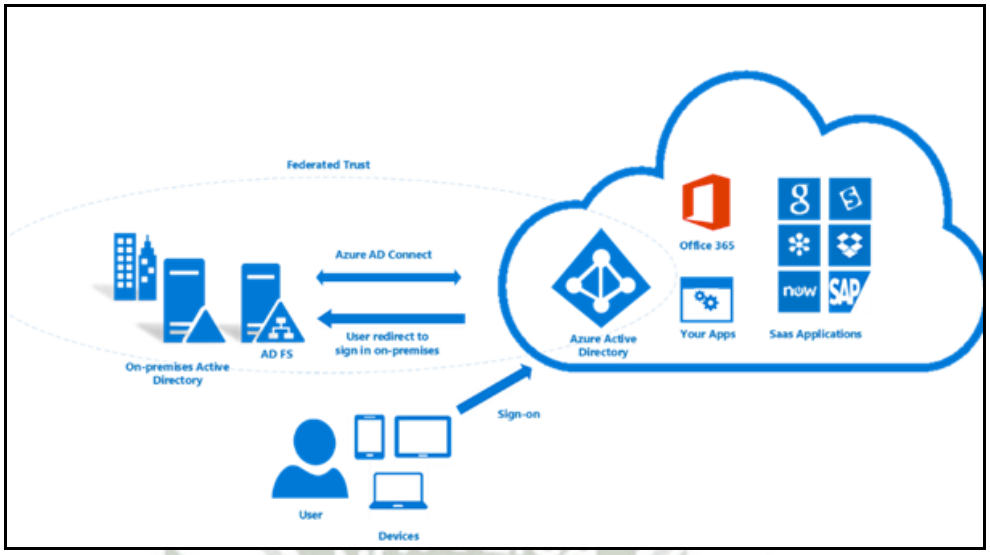


Fuente: Elaboración Propia

1.3.2.3.3 Modelo de Servicio SaaS

Software como Servicio (SaaS) (Figura 3), es una solución de software integrado ofrecido por un proveedor de servicios en la nube como lo son los aplicativos empresariales CRM (Administración de las relaciones con el cliente) y ERP (Planeamiento de recursos empresariales), donde el proveedor es el que administra el hardware y el software, donde el costo es únicamente por el uso. (Murazzo, 2016).

Figura 3: Arquitectura del servicio SaaS



Fuente: Documentación Microsoft Azure

1.4 Técnicas y Herramientas

1.4.1 Técnicas

La implementación del proyecto procedió de la siguiente forma:

1.4.1.1 Etapa Inicial

- Evaluación y recolección de datos de infraestructura local de la institución.
- Dimensionamiento de los aplicativos.
- Diseño de arquitectura para los aplicativos.
- Creación de suscripción en Azure perteneciente a la institución.

1.4.1.2 Primera Etapa

- Creación y segmentación de redes en la nube.
- Implementación de 4 servidores (2 servidores web, 2 servidores para base de datos).

- Creación y configuración de balanceadores de carga.
- Configuración de grupo de seguridad para los accesos a servidores.
- Habilitación del entorno Power BI para poder visualizar el consumo y el costo respectivo de los componentes creados.

1.4.1.3 Segunda Etapa

- Se debe contar con escenarios de Alta Disponibilidad, asegurando el Nivel de Servicio (SLA) solicitado por la entidad.
- Este servicio soportará versiones de Windows Server 2012 y superior, Microsoft SQL Server 2012 y superior.
- La creación de capacidades adicionales (“máquinas virtuales”) se encuentran dentro del mismo segmento de red, o VLAN, para evitar restricciones a nivel de puertos y permitir desde el primer momento, que las máquinas virtuales estén desplegadas en su entorno de trabajo en su mismo segmento.

1.4.1.4 Capacidades

Las capacidades brindadas se encuentran bajo el modelo IaaS a la institución, la cual permite entre otras la creación de máquinas virtuales o físicas, ver el estado de los servicios, etc.

La institución obtendrá el servicio que precisa en materia de capacidad de procesamiento, almacenamiento (espacio), capacidad de red (ancho de banda) y sistemas operativos en una infraestructura a la que accede para su administración, a través de internet con conexiones seguras mediante enlaces y/o túneles, con las siguientes especificaciones:

- Despliegue de máquinas virtuales además de base de datos en alta disponibilidad.
- Contar con roles y/o plantillas pre diseñados para desplegar capacidades de acuerdo a la necesidad.
- El tiempo de recuperación ante una falla en la infraestructura base no deberá exceder el tiempo establecido en los niveles de servicio.
- Toda la solución requerida debe contar con mecanismos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

1.4.2 Herramientas

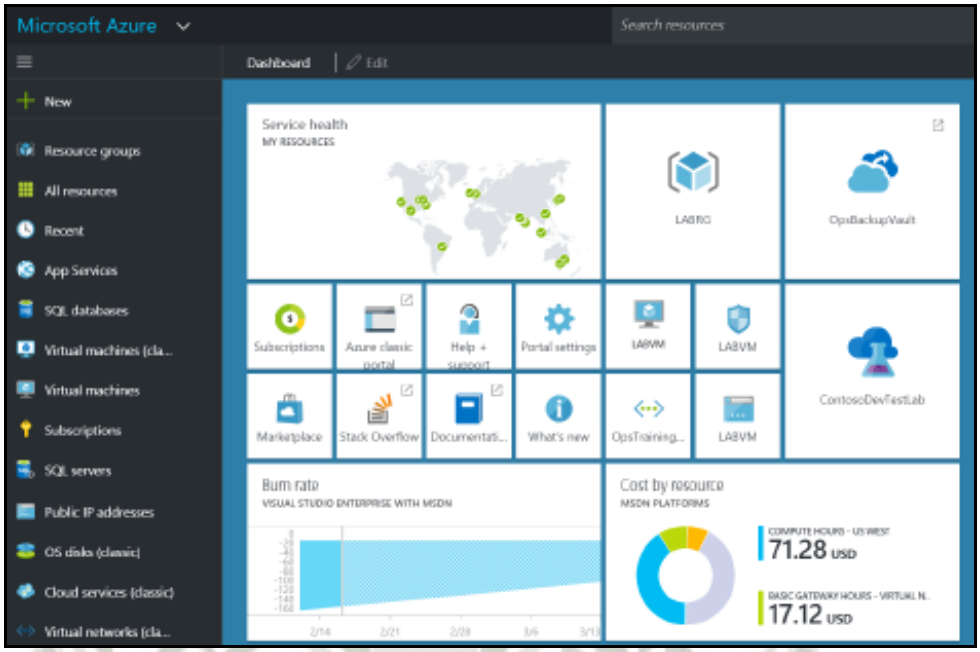
1.4.2.1 Azure

El servicio en la nube de Azure admite tecnologías las cuales son utilizadas por millones de desarrolladores y profesionales de TI (Figura 4), es por eso que se integra fácilmente con su entorno de TI actual a través de la mayor red de conexiones privadas seguras, soluciones de base de datos y almacenamiento híbridos, así como funciones de residencia y cifrado de datos, de forma que sus activos permanecen justo donde los necesita. Este es el motivo por el que es uno de los mejores servicios de informática en la nube disponibles.

El servicio de uso se puede escalar o reducir verticalmente con rapidez para adaptarse a la demanda.

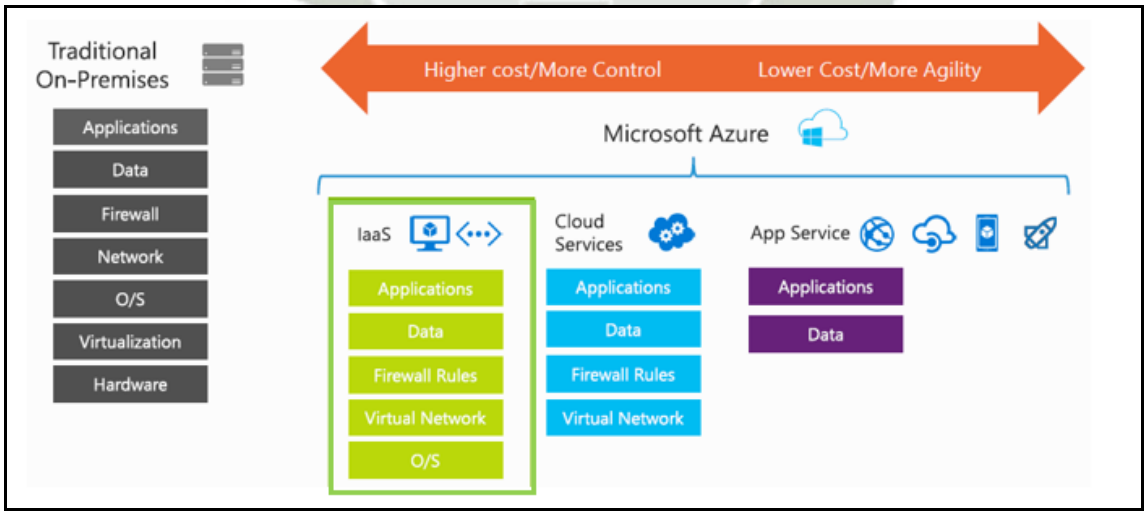
La legitimidad e integridad de los datos almacenados en la nube es un requerimiento las diferentes empresas con respecto a sus migraciones es por eso que Microsoft ha adoptado un compromiso líder en el sector de proteger sus datos y su privacidad (Figura 5).

Figura 4: Interfaz de Plataforma Azure



Fuente: Microsoft Azure

Figura 5: Estructura de la Plataforma Azure



Fuente: Documentación Microsoft Azure

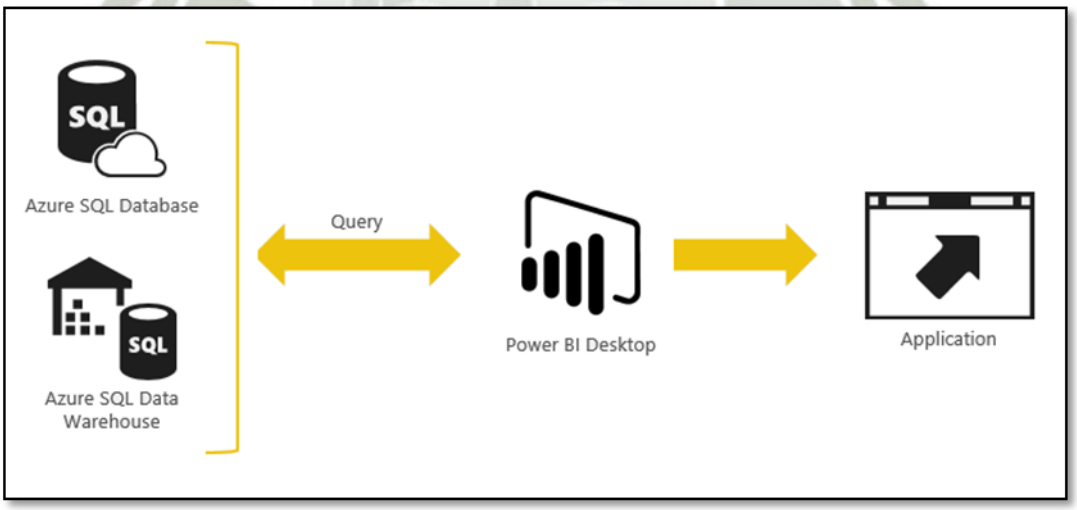
1.4.2.2 Power BI

Power BI es un conjunto de aplicaciones de análisis de negocios que permite analizar datos y compartir información. Los paneles de Power BI ofrecen a los usuarios una vista completa con sus métricas más importantes en un mismo lugar. (Figura 6)

La información se actualiza en tiempo real y está disponible en todos sus dispositivos. La creación de un panel es una sencilla operación gracias a las más de 50 conexiones a conocidas aplicaciones empresariales, que se completan con paneles pre generados y diseñados por expertos para ayudarle a ponerse en marcha rápidamente.

Proporciona informes y análisis la organización, permite alcanzar la máxima productividad en las tareas definidas. Power BI puede unificar todos los datos de la organización, ya sea en la nube o localmente.

Figura 6: Escenario de Conexión con Azure



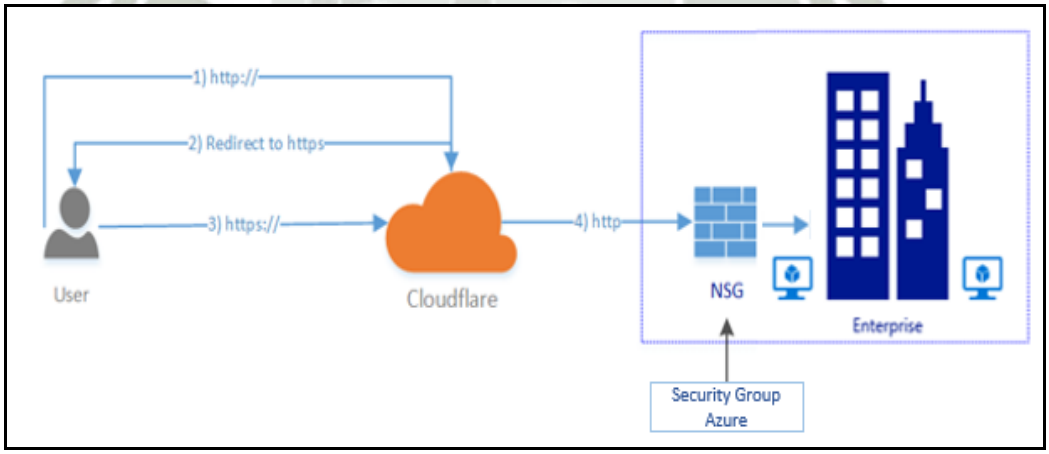
Fuente: Documentación Power BI

1.4.2.3 Cloudflare

Cloudflare es un proxy cuya función es agilizar y proteger sitios web, APIs y servicios de SaaS. Su tecnología Anycast permite que el rendimiento, la seguridad, fiabilidad y analítica que ofrecen mejore con cada servidor que se añade a su centro de datos (Figura 7).

Sus características principales para la protección de sitios web son con una WAF de grado empresarial y la protección contra ataques DDOS, del mismo modo para garantizar la respuesta en un tiempo mínimo a las solicitudes de acceso utiliza CDN que distribuye el contenido por el mundo para poder estar más cerca a los visitantes. Cloudflare maneja uno de los servicios DNS más rápidos de manera global, seguro y potente.

Figura 7: Escenario de Conexión con Azure



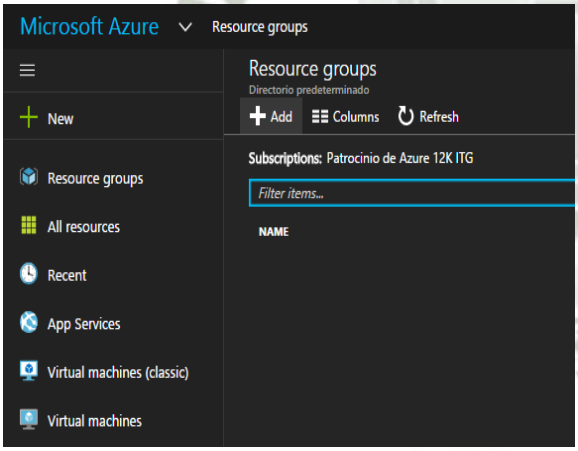
Fuente: Elaboración Propia

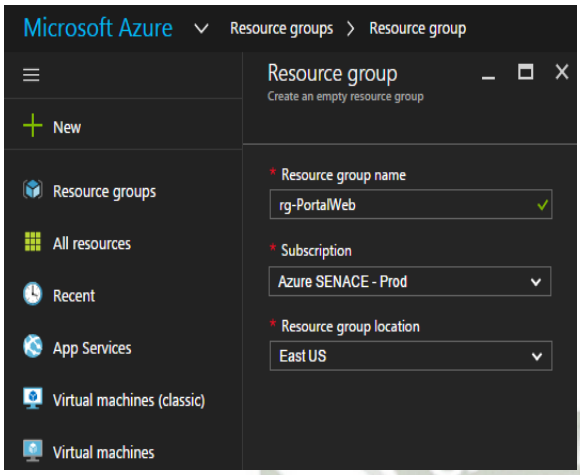
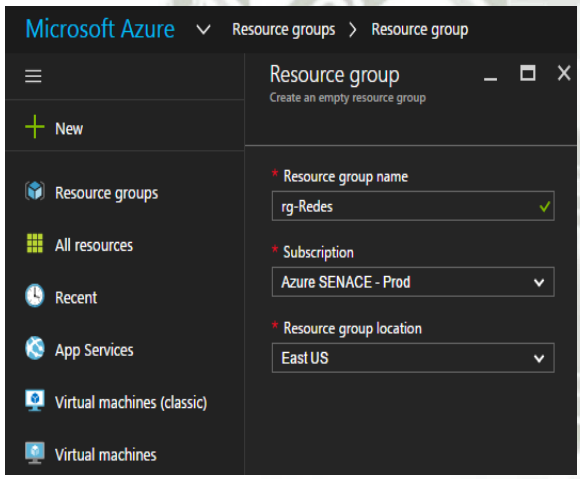
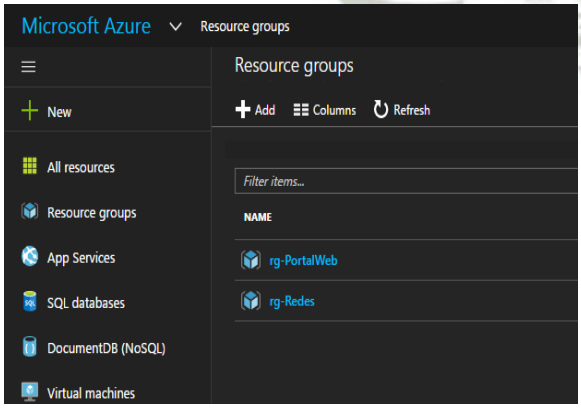
1.5 Aspectos Relevantes del Desarrollo

A continuación, se describe los pasos necesarios para la construcción del entorno en la plataforma de Azure en la cual se alojará el Portal Web de la institución, que brindará una alta disponibilidad a nivel de servidores y base de datos, así como también balanceo de carga en los servidores web y de base datos para un mejor rendimiento.

1.5.1 Resource Group

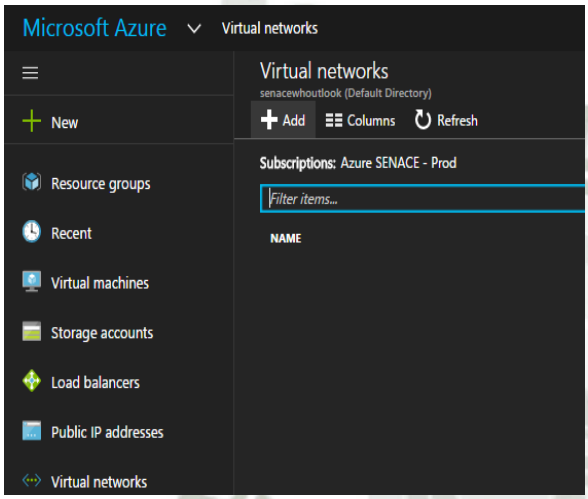
Tabla 01: Creación de Resource Group

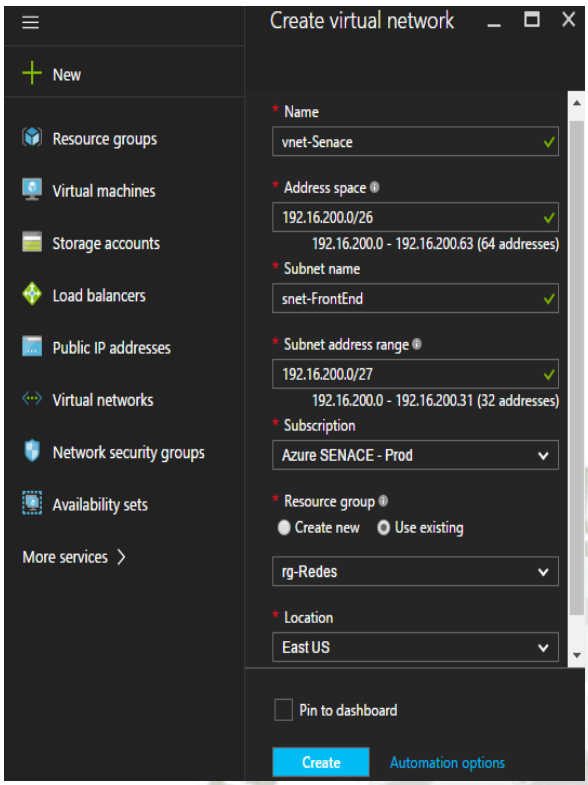
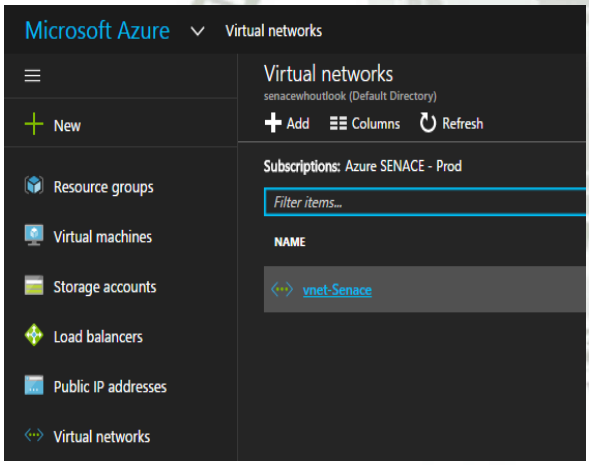
Ventana	Acción
	Se procederá a realizar la creación de los **Resource Group** que albergaran los componentes de Microsoft Azure.
	Seleccionar **Resource Group > Add**

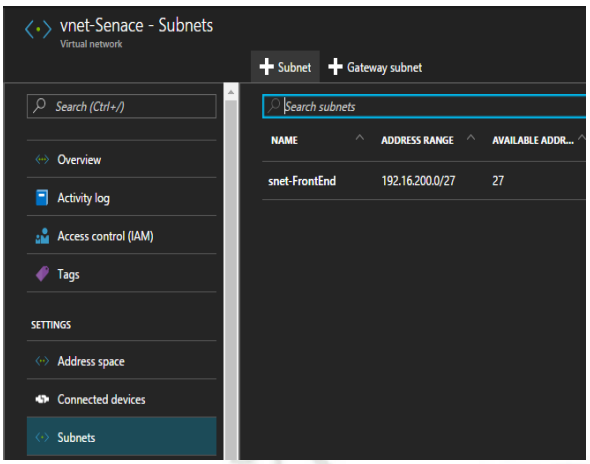
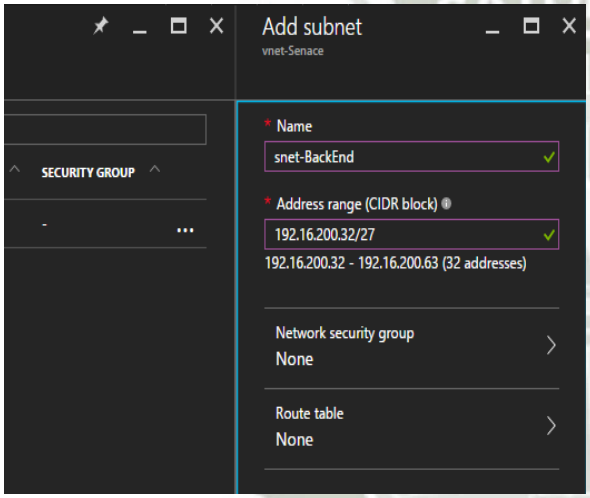
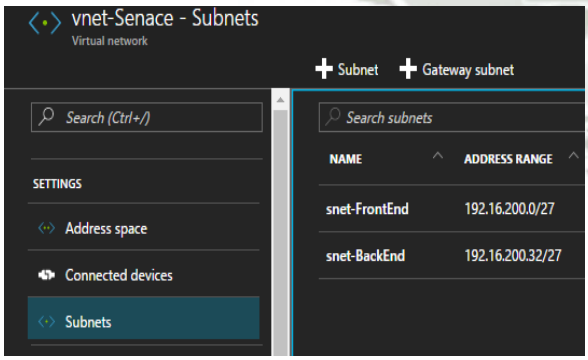
Ventana	Acción
	Para la creación de un **Resource Group,** completar los siguientes campos: • **Resource Group:** rg-PortalWeb • **Subscription:** Azure SENACE – Prod • **Resource group location:** East US Seleccionar **Create.**
	Para la creación del segundo **Resource Group,** completar los siguientes campos: • **Resource Group:** rg-Redes • **Subscription:** Azure SENACE – Prod • **Resource group location:** East US Seleccionar **Create.**
	Al finalizar, podemos visualizar los **Resource Group** creados: • rg-PortalWeb • rg-Redes

1.5.2 Virtual Network y Subnet

Tabla 2: Creación de IP Public

Ventana	Acción
	Se procederá a realizar la creación de la **Virtual Network** y **Subnets**.
	Seleccionar **Virtual networks > Add**

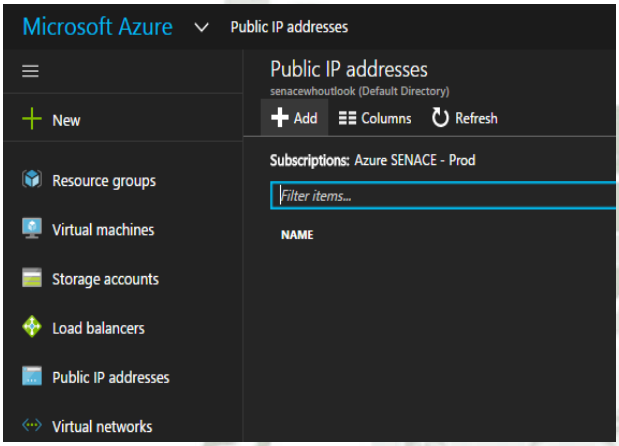
Ventana	Acción
	Para realizar la creación de la **Virtual network** y primera **subnet**, completar los siguientes campos: • **Name:** vnet-Senace • **Address space:** 192.16.200.0/26 • **Subnet name:** snet-FrontEnd • **Subnet address range:** 192.16.200.0/27 • **Subscription:** Azure SENACE – Prod • **Resource group:** rg-Redes • **Location:** East US Seleccionar **Create.**
	Al finalizar, se visualiza la **virtual network** creada.

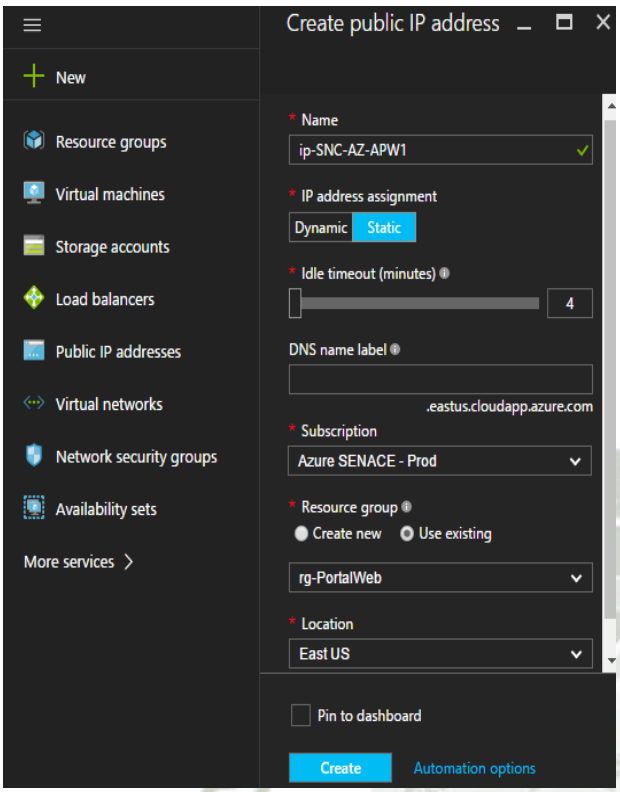
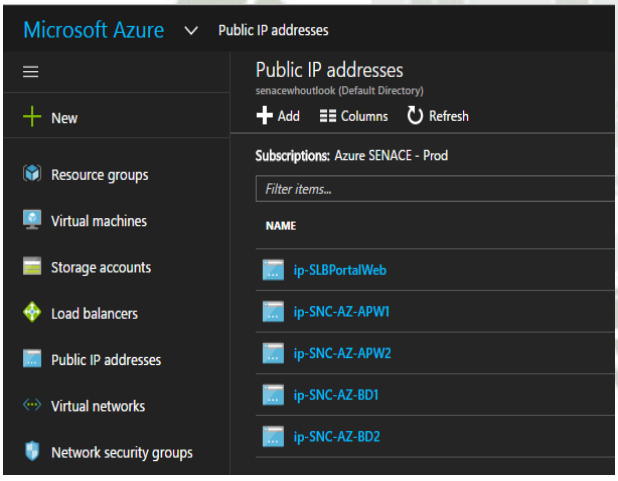
Ventana	Acción
	Asimismo se visualiza la **subnet** creada.
	Para la creación de la segunda **subnet**, completar los siguientes campos: • **Name:** snet-BackEnd • **Addressrange:** 192.16.200.32/27 • **Network security group:** None • **Route table:** None Seleccionar **Create**.
	Al finalizar, se visualiza la creación de las **subnets**.

Fuente: Elaboración Propia

1.5.3 IP Public

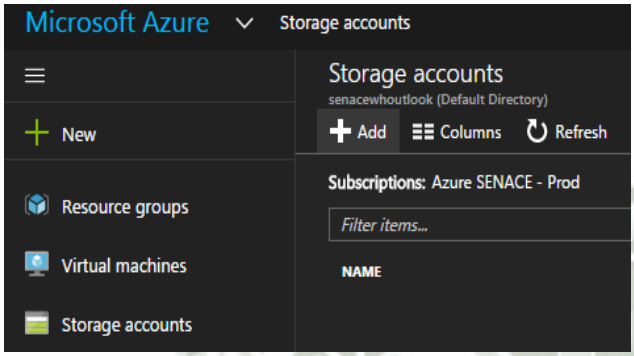
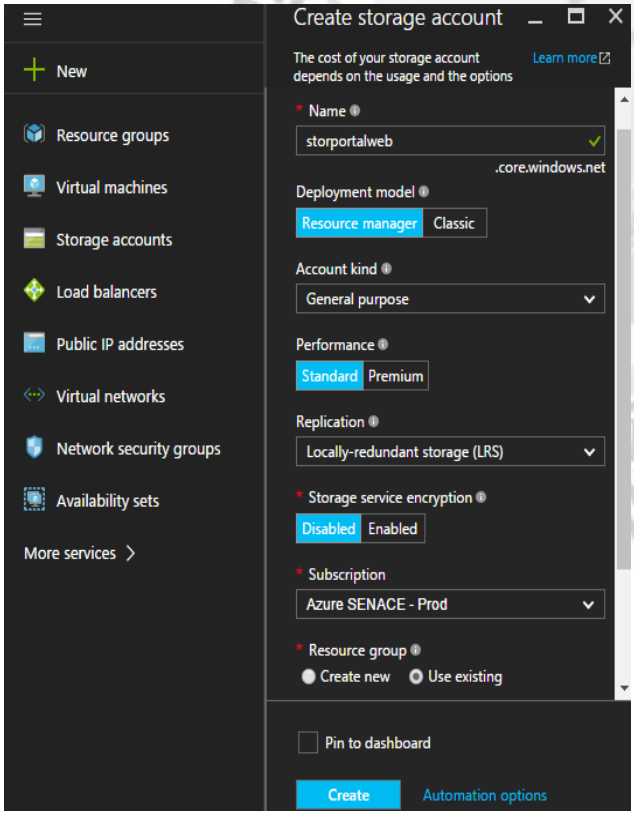
Tabla 3: Creación de Storage

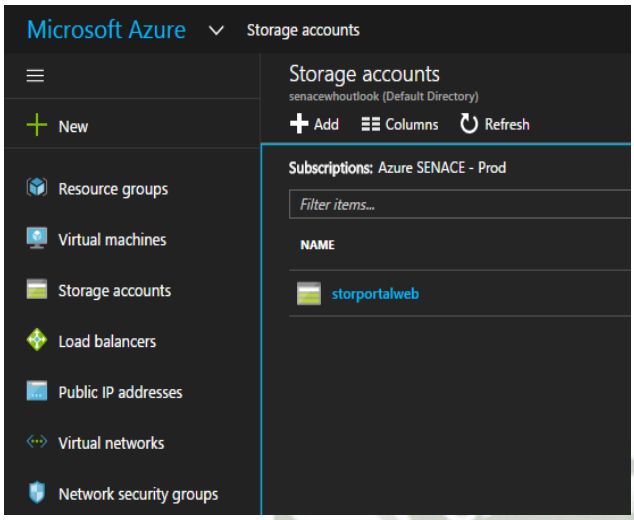
Ventana	Acción
	Procedemos con la creación de las **Public IP address** para nuestros servidores.
	Seleccionar **Public IP addresses** > **Add**

Ventana	Acción
	Para realizar la creación de la **public IP address**, completar los siguientes campos: • **Name:** ip-SNC-AZ-APW1 • **IP address assignment:** Static • **Idle timout (minutes):** 4 • **Subscription:** Azure SENACE – Prod • **Resource group:** rg-Portal Web • **Location:** East US Seleccionar **Create**.
	Repetimos los mismos pasos para la creación de las otras **Public IP address** de los servidores, las cuales son: • **ip-SNC-AZ-APW1** • **ip-SNC-AZ-APW2** • **ip-SNC-AZ-BD1** • **ip-SNC-AZ-BD2**

Fuente: Elaboración Propia

1.5.4 Storage

Ventana	Acción
	Proseguimos con la creación del **Storage accounts** para el almacenamiento de discos de data y sistema operativo.
	Seleccionar **Storage accounts** > **Add**
	Para realizar la creación del **Storage account**, completar los siguientes campos: • **Name:** storportalweb • **Deployment model:** Resource manager • **Account kind:** General purpose • **Performance:** Standard • **Replication:** Locally-redundant storage (LRS) • **Storage service encryption:** Disabled • **Subscription:** Azure SENACE - Prod • **Resource Group:** rg-Portal Web Seleccionar **Create.**

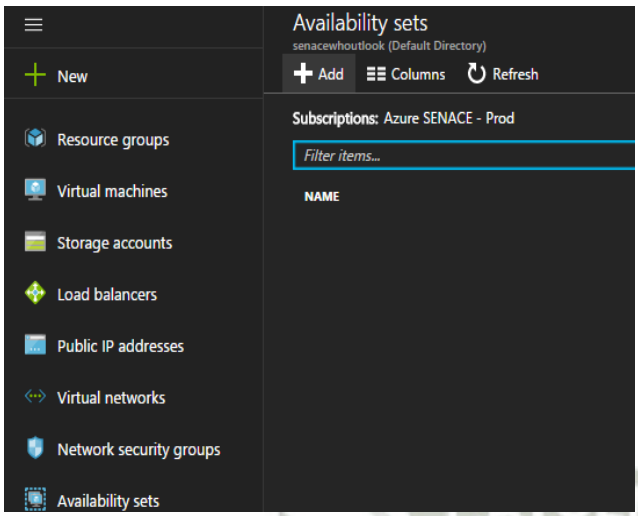
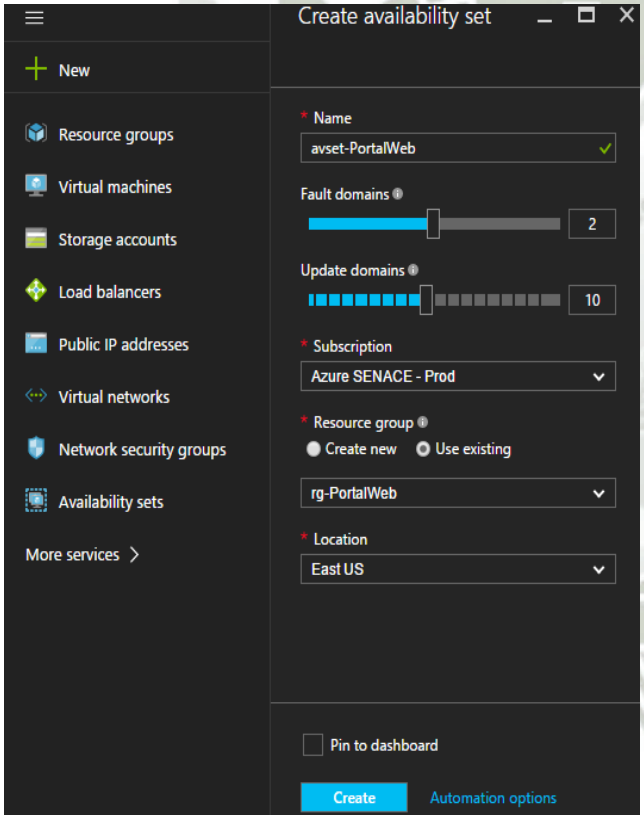
Ventana	Acción
	Al finalizar, se visualiza el **storage account** creado.

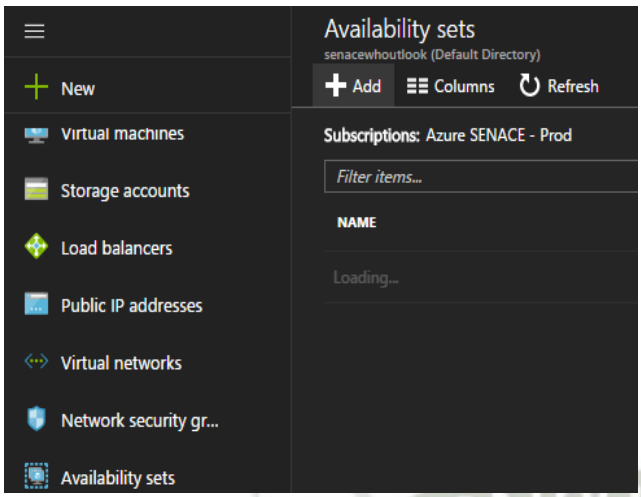
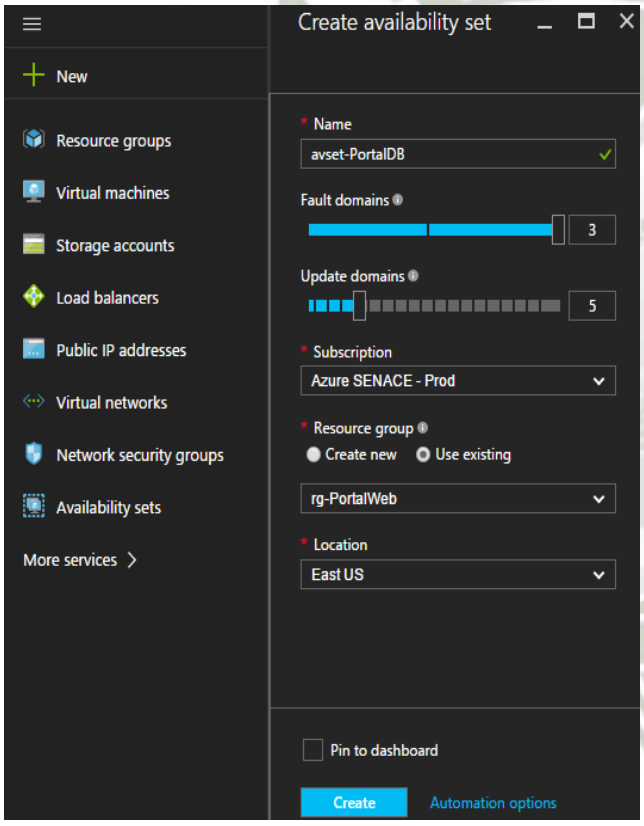
Fuente: Elaboración Propia

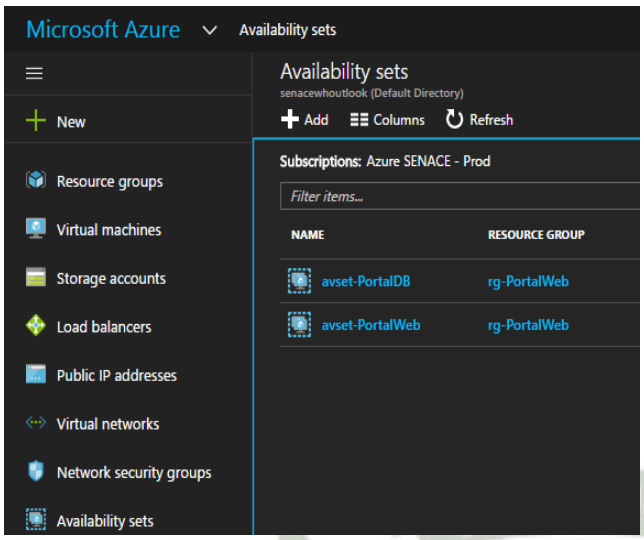
1.5.5 Availability Set

Tabla 4: Creación de los Availability Sets

Ventana	Acción
	Proseguimos con la creación del **availability set.**

Ventana	Acción
	Seleccionar **Availability sets > Add**
	Para realizar la creación del **Availabilitysets**, completar los siguientes campos: • **Name:** avset-PortalWeb • **Fault domains:** 2 • **Update domains:** 10 • **Subscription:** Azure SENACE -Prod • **Resource Group:** rg-Portal Web • **Location:** East US Seleccionar **Create.**

Ventana	Acción
	Para la creación del segundo **Availability Set** seleccionar **Add**.
	Para la creación del segundo **Availability set,** completar los siguientes campos: • **Name:** avset-PortalDB • **Fault domains:** 3 • **Update domains:** 5 • **Subscription:** Azure SENACE -Prod • **Resource group: rg-Portal Web** • **Location:** East US Seleccionar **Create.**

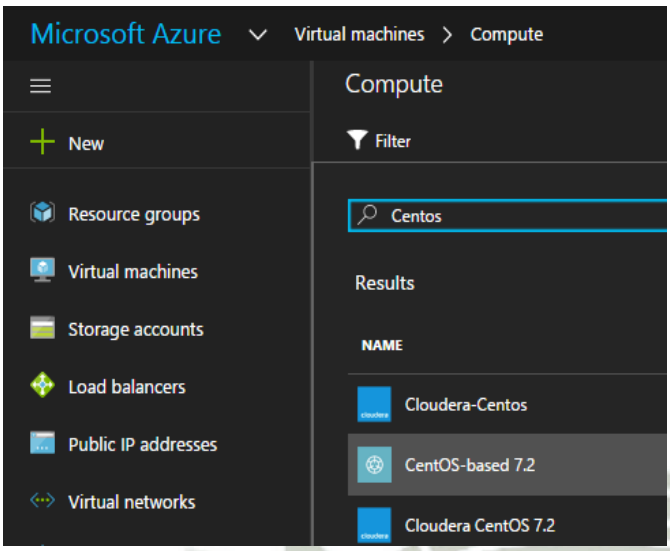
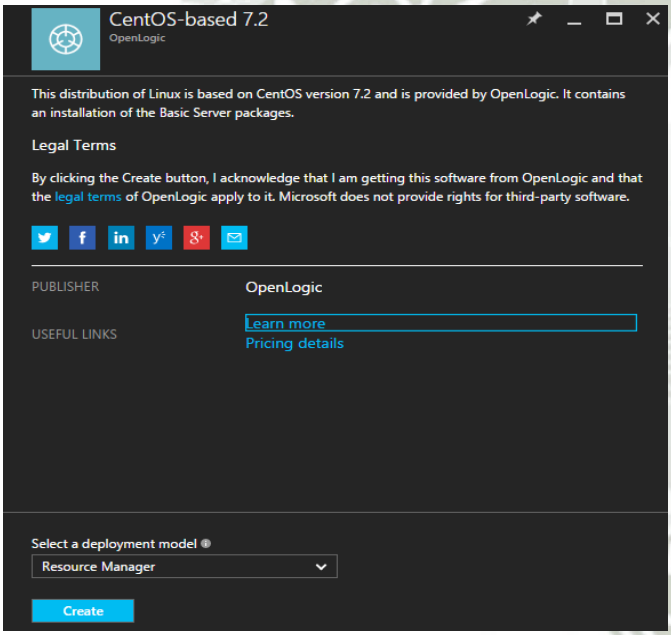
Ventana	Acción
	Al finalizar, se visualiza los **Availability Sets** creados.

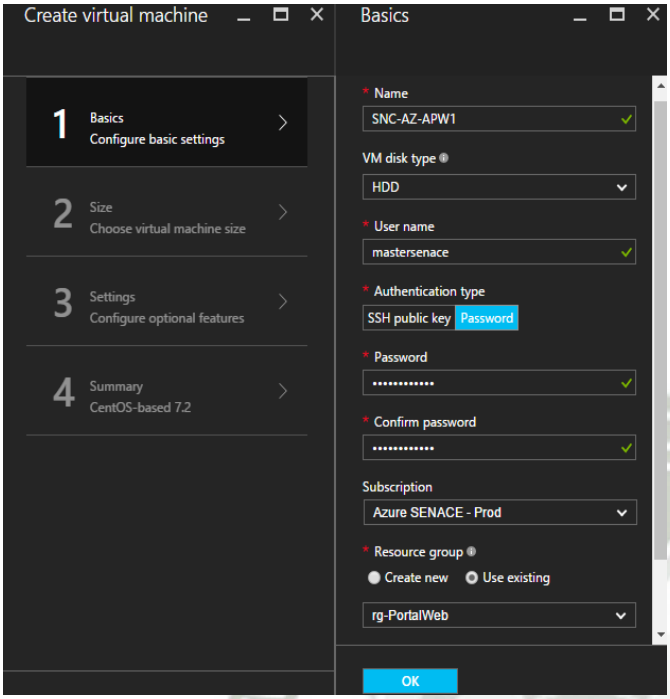
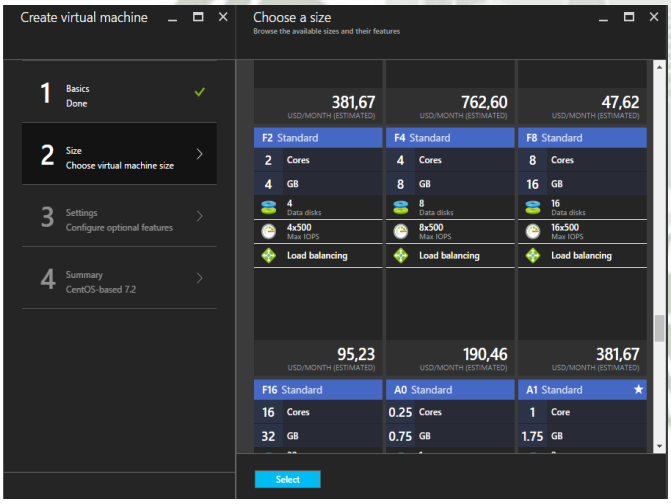
Fuente: Elaboración Propia

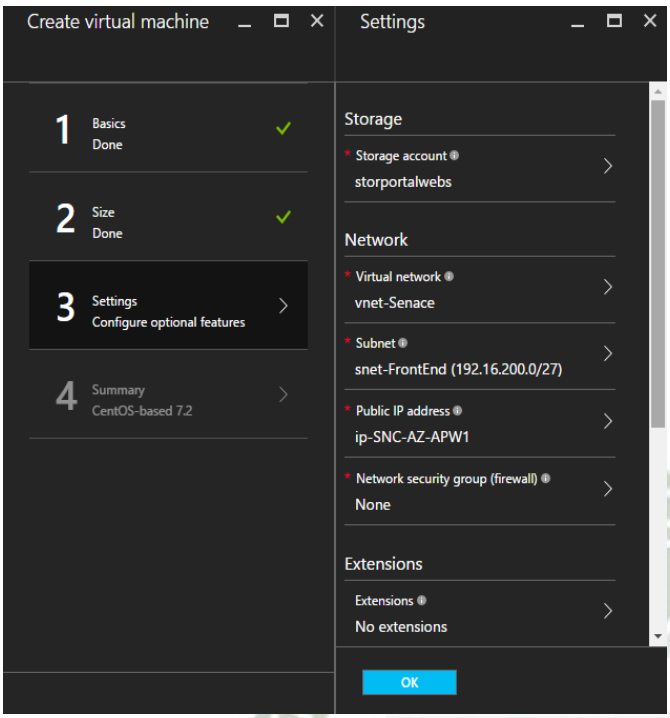
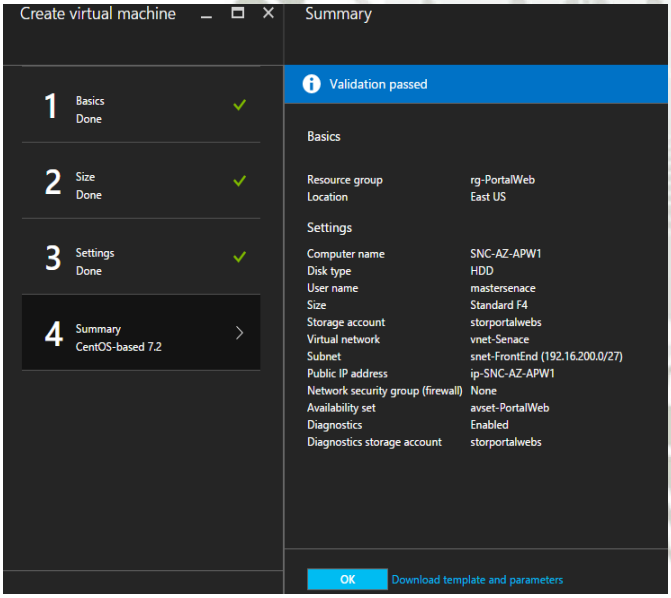
1.5.6 Virtual Machines

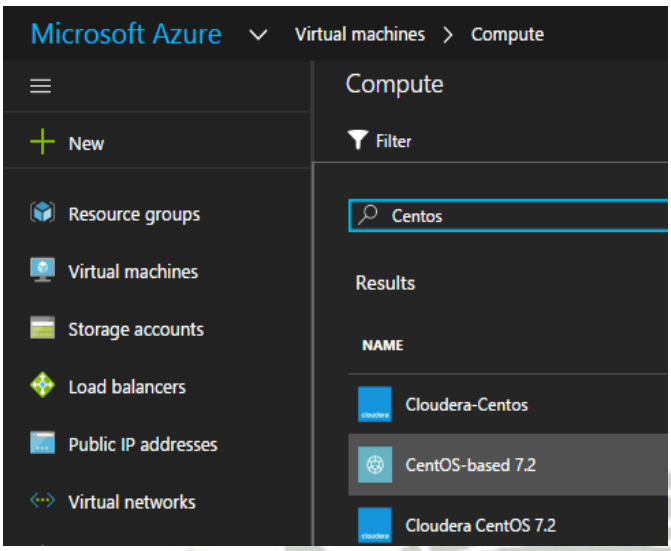
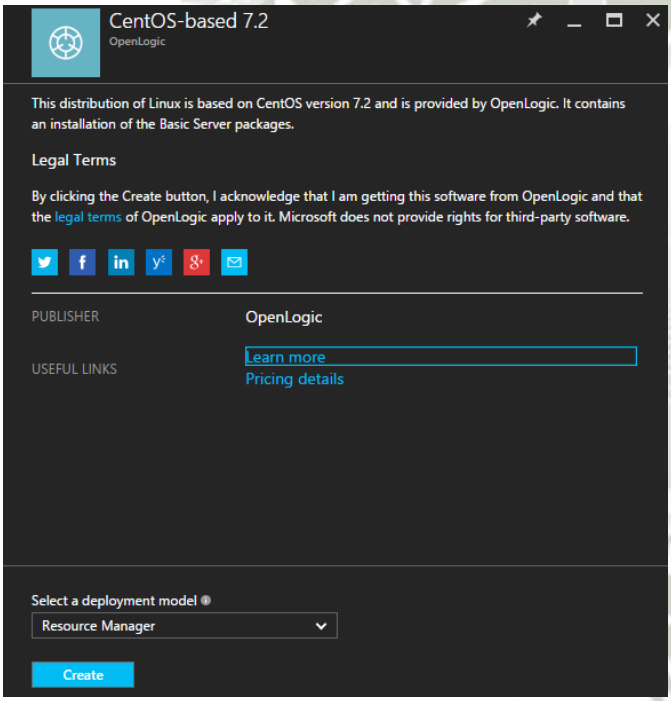
Tabla 5: Creación de Virtual Machine

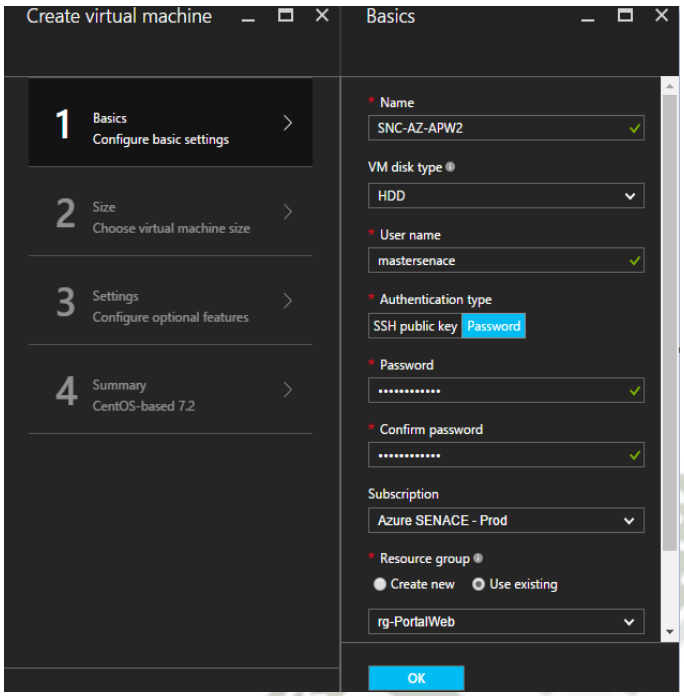
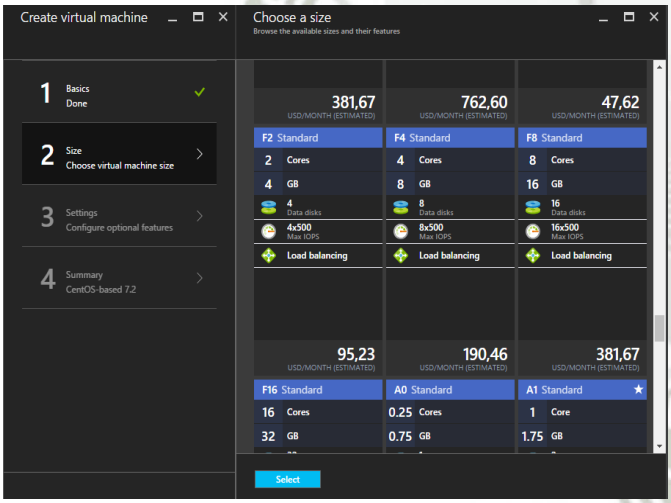
Ventana	Acción
	Continuamos con la creación del primer servidor web: **SNC-AZ-APW1**

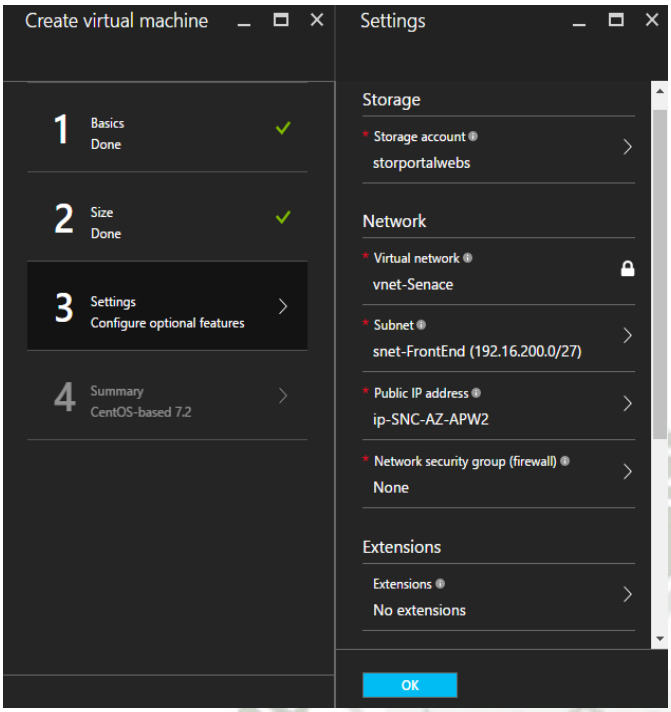
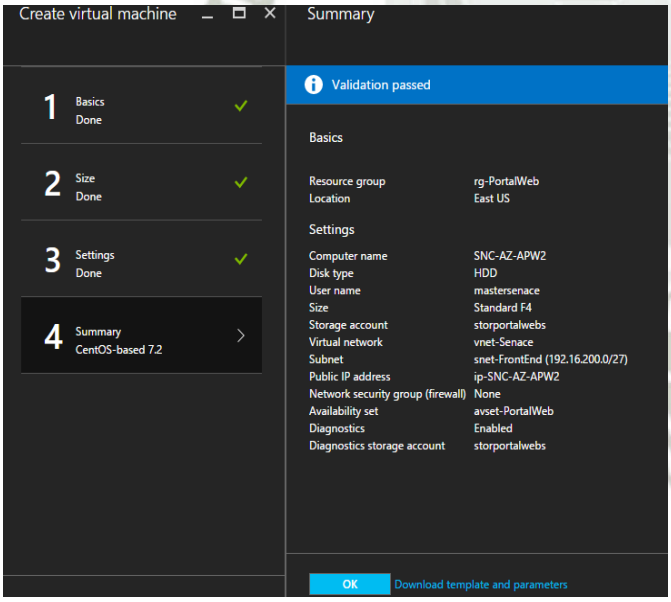
Ventana	Acción
	Para la creación de una máquina virtual, seleccionar **CentOS – based 7.2**
	En la sección **Select a deployment model**, seleccionar **Resource Manager > Create.**

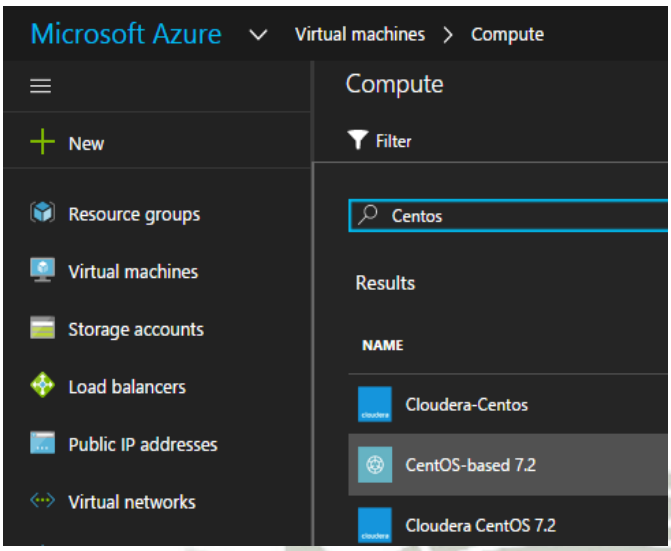
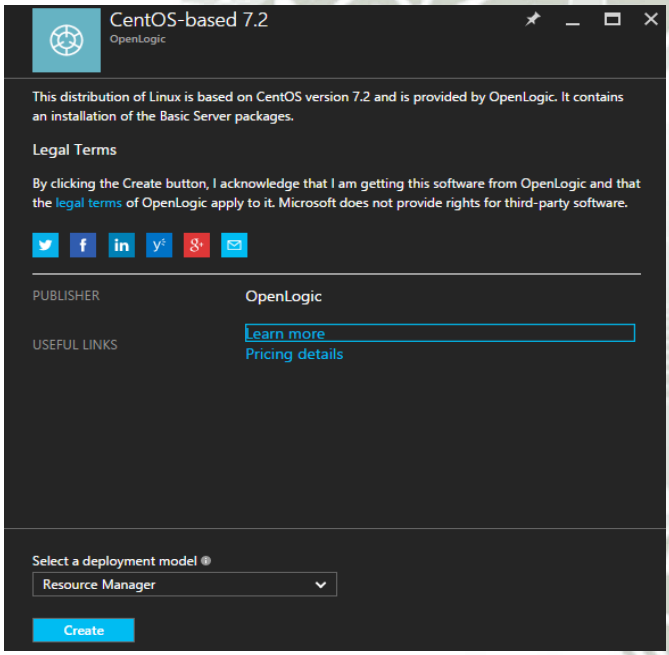
Ventana	Acción
	Para realizar la creación de la primera máquina virtual, completar los siguientes campos: • **Name:** SNC-AZ-APW1 • **VM disk type:** HDD • **User name:** mastersenace • **Authentication type:** Password • **Subscription:** Azure SENACE - Prod • **Resource Group:** rg-Portal Web • **Availability Set:** avset-PortalWeb • **Monitoring:** Enabled Seleccionar **Create**.
	En la sección **Size**, seleccionamos el tamaño de nuestra máquina virtual, serie **F4**

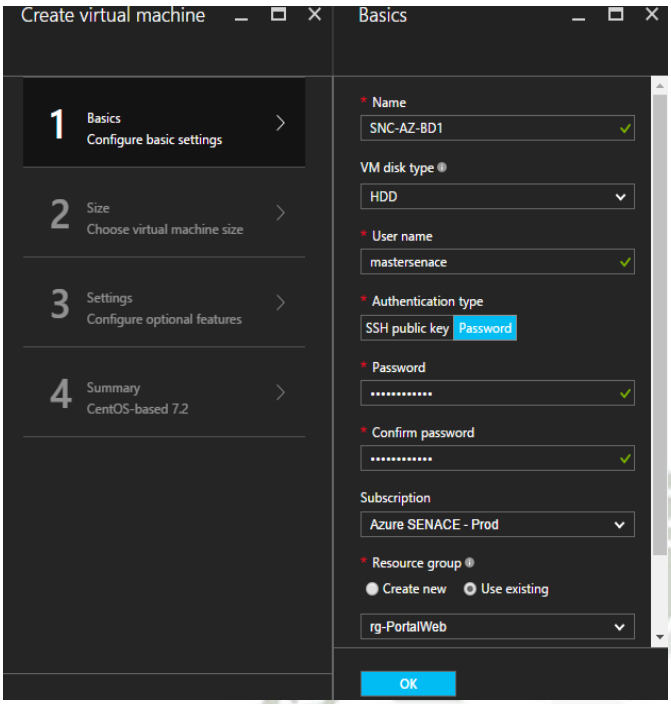
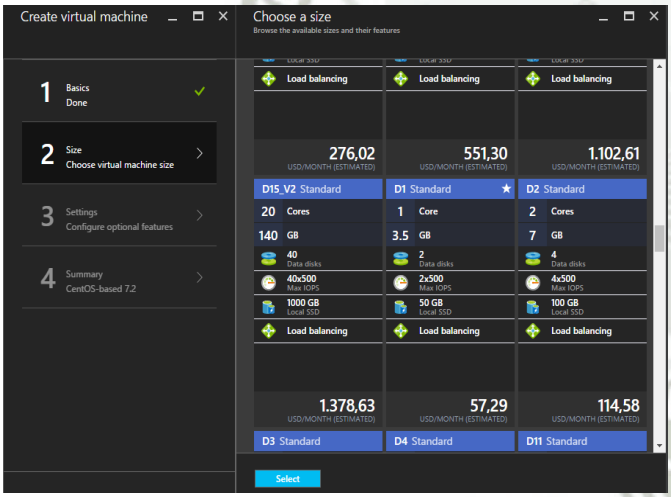
Ventana	Acción
	En la sección **Settings**, selecciones los siguientes campos: • **Storage account:** storportalweb • **Virtual network:** vnet-Senace • **Subnet:** snet-FrontEnd • **Public IP address:** ip-SNC-AZ-APW1 • **Network security group:** none Seleccionar **OK.**
	En la sección **Summary**, validamos que los datos sean correctos. Seleccionar **OK.**
	Continuamos con la creación del segundo servidor web: **SNC-AZ-APW2**

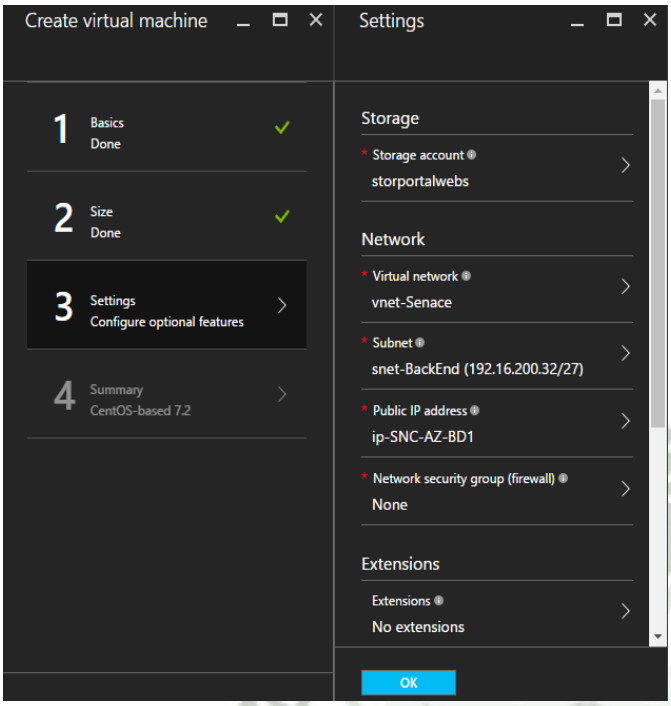
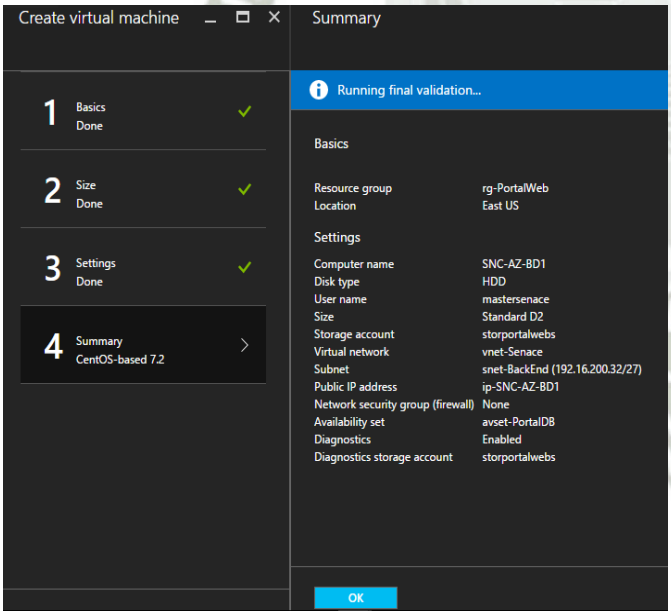
Ventana	Acción
	Para la creación de una máquina virtual, seleccionar **CentOS – based 7.2**
	En la sección **Select a deployment model**, seleccionar **Resource Manager > Create**

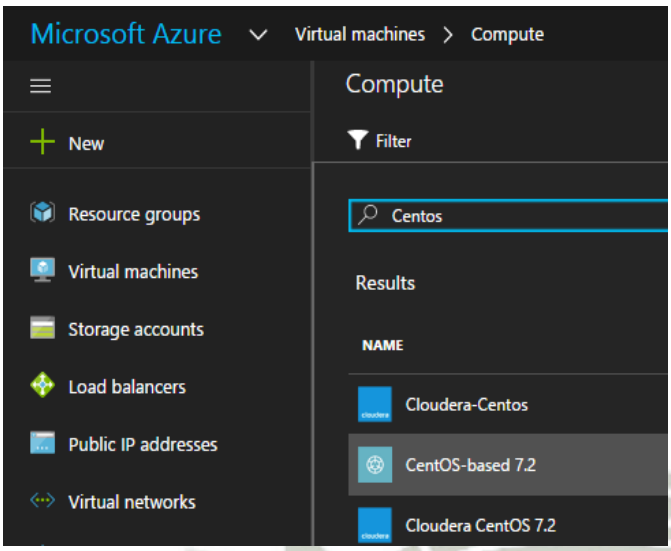
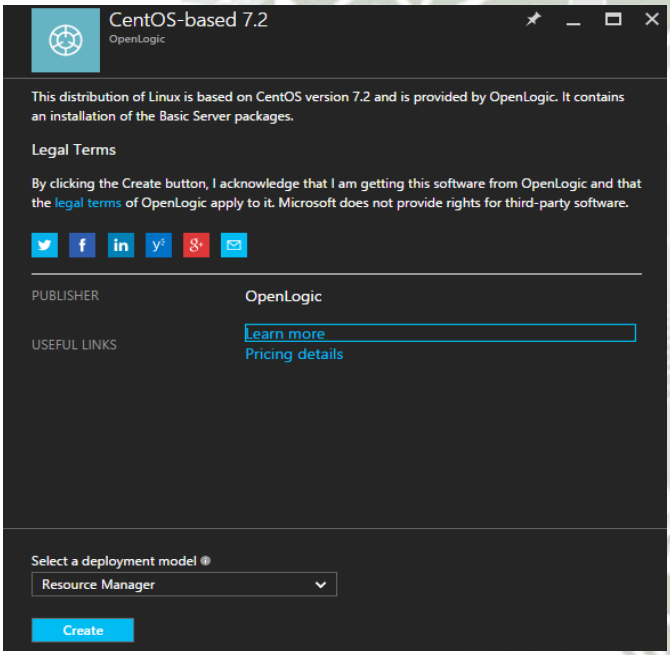
Ventana	Acción
	Para realizar la creación de la segunda máquina virtual, completar los siguientes campos: • **Name:** SNC-AZ-APW2 • **VM disk type:** HDD • **User name:** mastersenace • **Authentication type:** Password • **Subscription:** Azure SENACE - Prod • **Resource Group:** rg-Portal Web Seleccionar **Create**.
	En la sección **Size**, seleccionamos el tamaño de nuestra máquina virtual, serie **F4.**

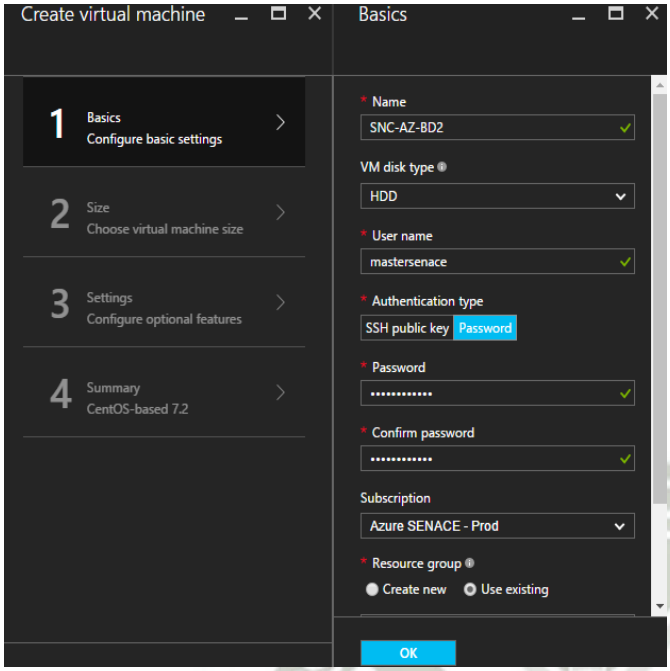
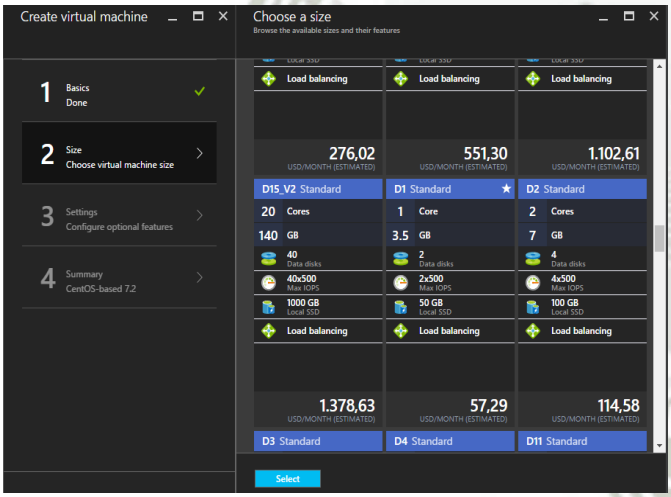
Ventana	Acción
	En la sección **Settings**, selecciones los siguientes campos: • **Storage account:** storportalweb • **Virtual network:** vnet-Senace • **Subnet:** snet-FrontEnd • **Public IP address:** ip-SNC-AZ-APW2 • **Network security group:** none • **Availability Set:** avset-PortalWeb • **Monitoring:** Enabled Seleccionar **OK.**
	En la sección **Summary**, validamos que los datos sean correctos. Seleccionar **OK.**
	Continuamos con la creación del primer servidor de base de datos: **SNC-AZ-BD1**

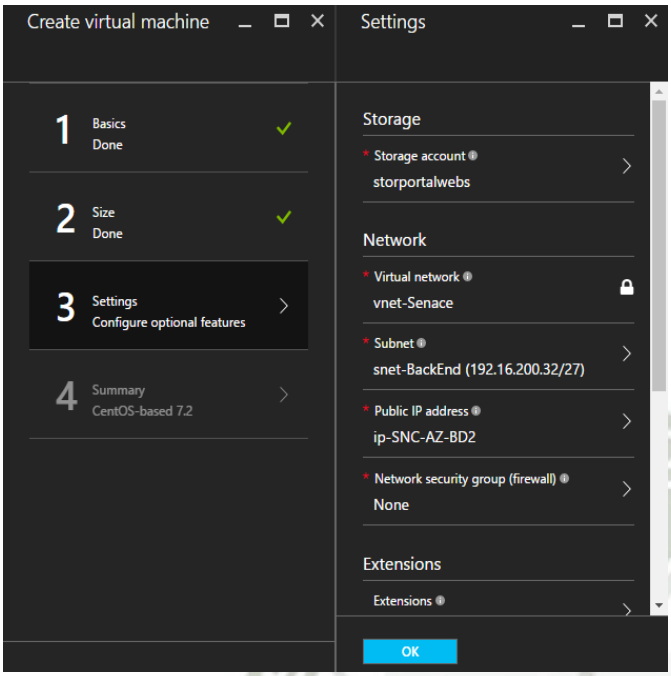
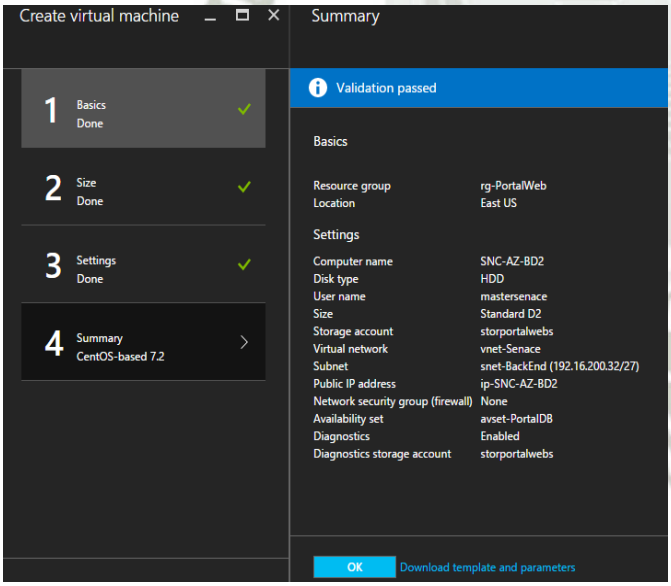
Ventana	Acción
	Para crear la **VM** elegimos el tipo que en este caso será **CentOS – based 7.2**
	En la sección **Select a deployment model**, seleccionar **Resource Manager > Create**

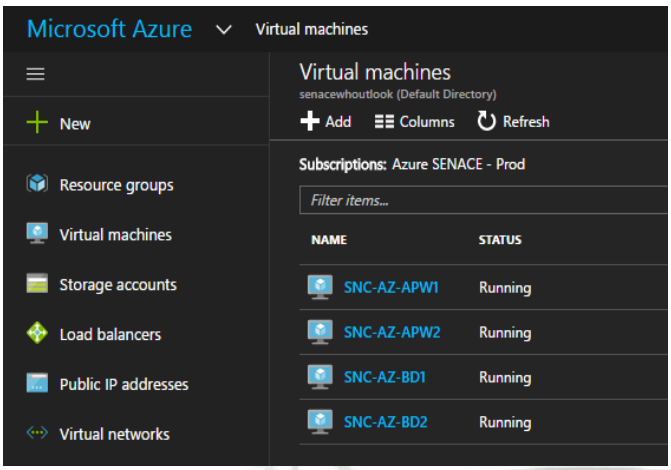
Ventana	Acción
	Para realizar la creación de la tercera máquina virtual, completar los siguientes campos: • **Name:** SNC-AZ-BD1 • **VM disk type:** HDD • **User name:** mastersenace • **Authentication type:** Password • **Subscription:** Azure SENACE - Prod • **Resource Group:** rg-Portal Web Seleccionar **Create**.
	En la sección **Size**, seleccionamos el tamaño de nuestra máquina virtual, serie **D2.**

Ventana	Acción
	En la sección **Settings**, selecciones los siguientes campos: • **Storage account:** storportalweb • **Virtual network:** vnet-Senace • **Subnet:** snet-BacktEnd • **Public IP address:** ip-SNC-AZ-BD1 • **Network security group:** none • **Availability Set:** avset-PortalDB • **Monitoring:** Enabled Seleccionar **OK.**
	En la sección **Summary**, validamos que los datos sean correctos. Seleccionar **OK.**
	Continuamos con la creación del segundo servidor de base de datos: **SNC-AZ-BD2**

Ventana	Acción
	Para la creación de una máquina virtual, seleccionar **CentOS – based 7.2**
	En la sección **Select a deployment model**, seleccionar **Resource Manager > Create**

Ventana	Acción
	Para realizar la creación de la tercera máquina virtual, completar los siguientes campos: • **Name:** SNC-AZ-BD2 • **VM disk type:** HDD • **User name:** mastersenace • **Authentication type:** Password • **Subscription:** Azure SENACE - Prod • **Resource Group:** rg-Portal Web Seleccionar **Create**.
	En la sección **Size**, seleccionamos el tamaño de nuestra máquina virtual, serie **D2.**

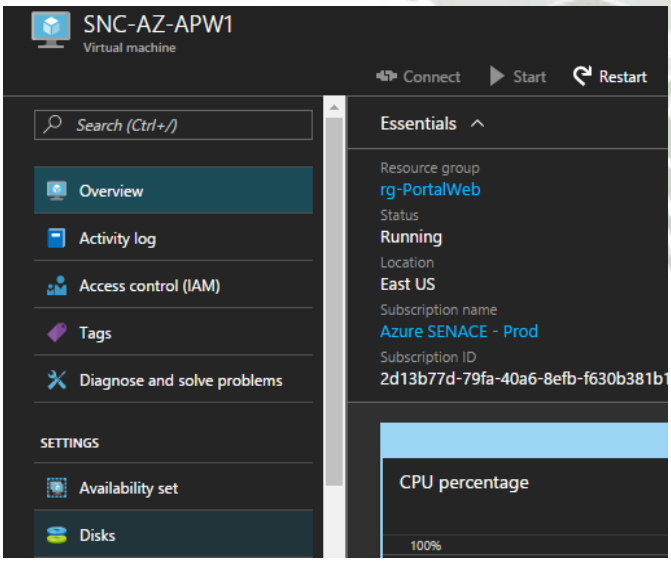
Ventana	Acción
	En la sección **Settings**, selecciones los siguientes campos: • **Storage account:** storportalweb • **Virtual network:** vnet-Senace • **Subnet:** snet-BacktEnd • **Public IP address:** ip-SNC-AZ-BD2 • **Network security group:** none • **Availability Set:** avset-PortalDB • **Monitoring:** Enabled Seleccionar **OK.**
	En la sección **Summary**, validamos que los datos sean correctos. Seleccionar **OK.**

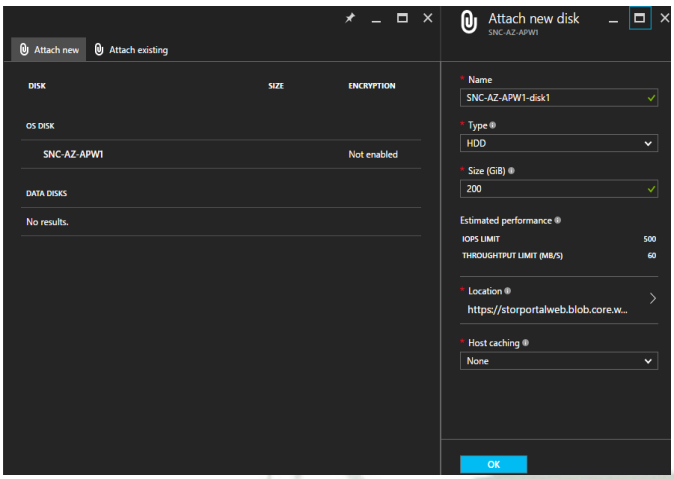
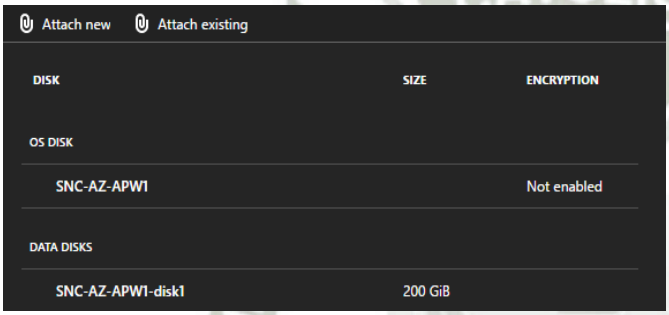
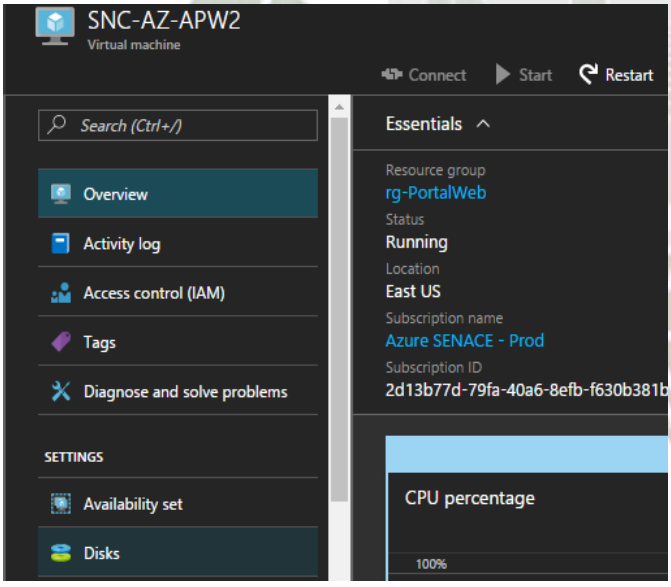
Ventana	Acción
	Al finalizar, visualizamos las 4 máquinas virtuales creadas.

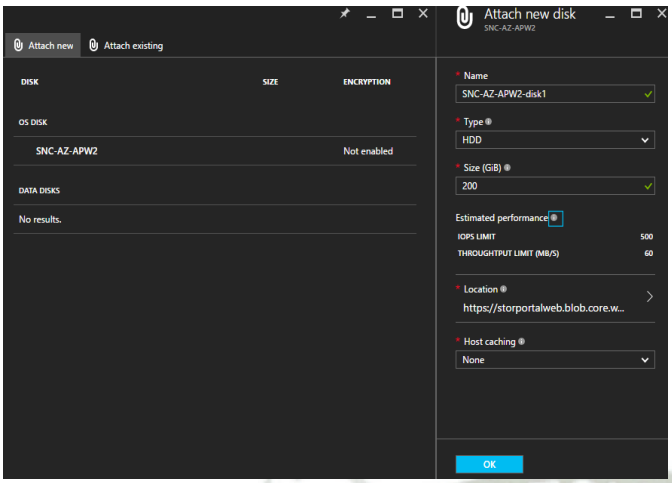
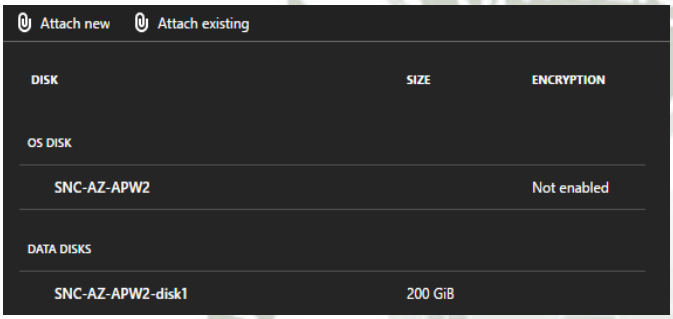
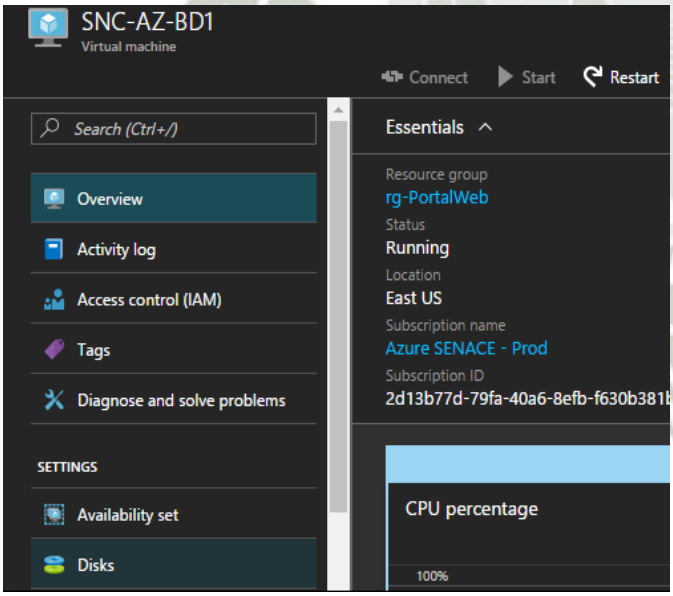
Fuente: Elaboración Propia

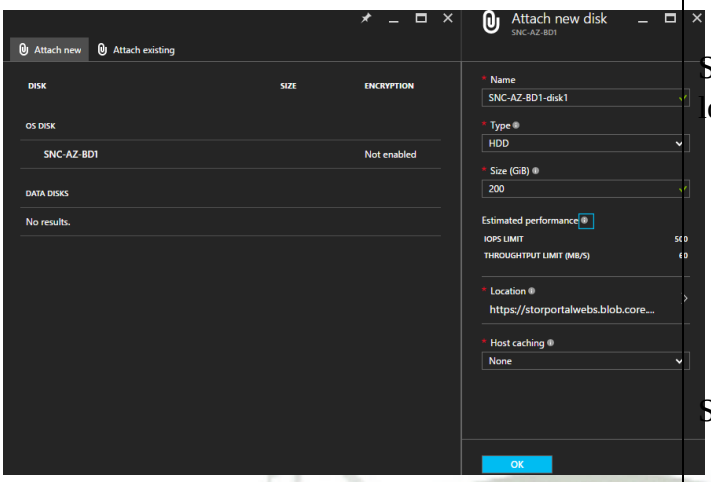
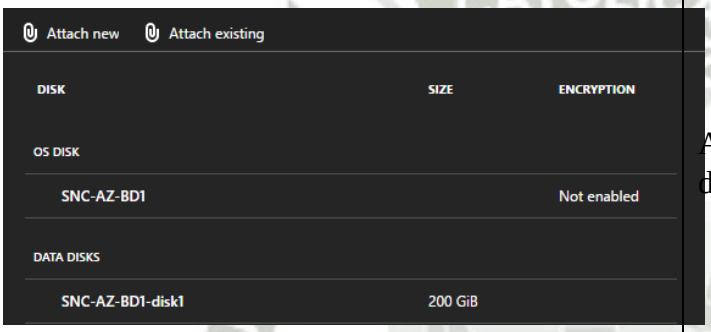
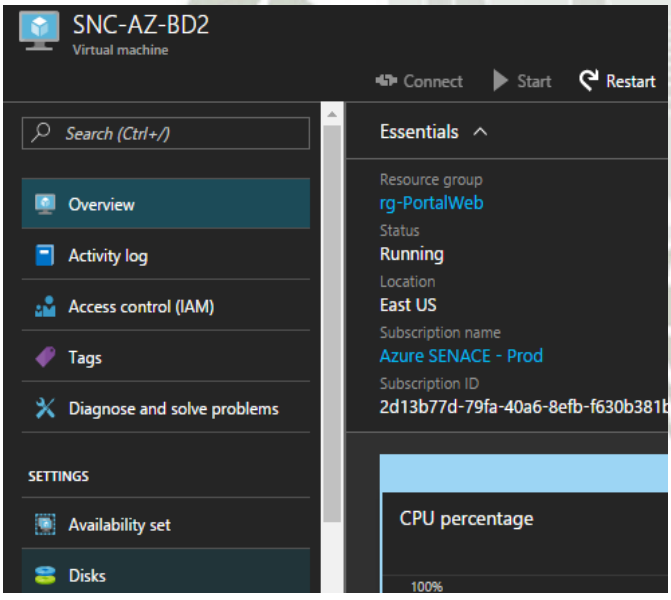
1.5.7 Attach Disk

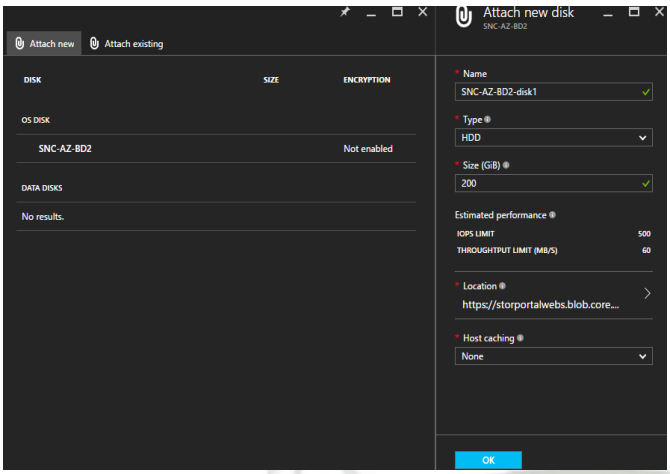
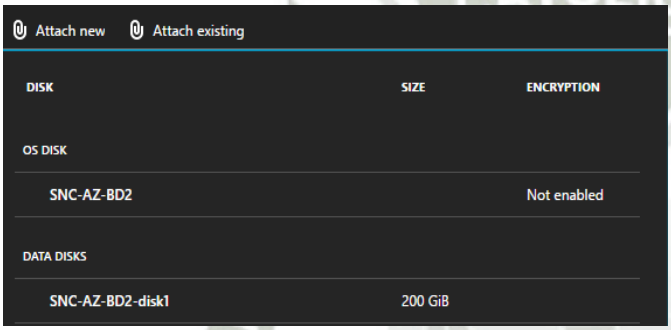
Tabla 6: Creación de discos

Ventana	Acción
	Continuamos con la configuración de los discos de las máquinas virtuales.
	Seleccionar **Virtual machine > SNC-AZ-APW1 > Disks**

Ventana	Acción
	Seleccionar **Attach new** y completar los siguientes campos: • **Name:** SNC-AZ-APW1-disk1 • **Type:** HDD • **Size:** 200 • **Host caching:** None Seleccionar **OK**
	Al finalizar, visualizamos el disco de datos creado.
	Seleccionar **Virtual machine > SNC-AZ-APW2 > Disks**

Ventana	Acción
	Seleccionar **Attach new** y completar los siguientes campos: • **Name:** SNC-AZ-APW2-disk1 • **Type:** HDD • **Size:** 200 • **Host caching:** None Seleccionar **OK**
	Al finalizar, visualizamos el disco de datos creado.
	Seleccionar **Virtual machine** > **SNC-AZ-BD1** > **Disks**

Ventana	Acción
	Seleccionar **Attach new** y completar los siguientes campos: • **Name:** SNC-AZ-BD1-disk1 • **Type:** HDD • **Size:** 200 • **Host caching:** None Seleccionar **OK**
	Al finalizar, visualizamos el disco de datos creado.
	Seleccionar **Virtual machine** > **SNC-AZ-BD2** > **Disks**

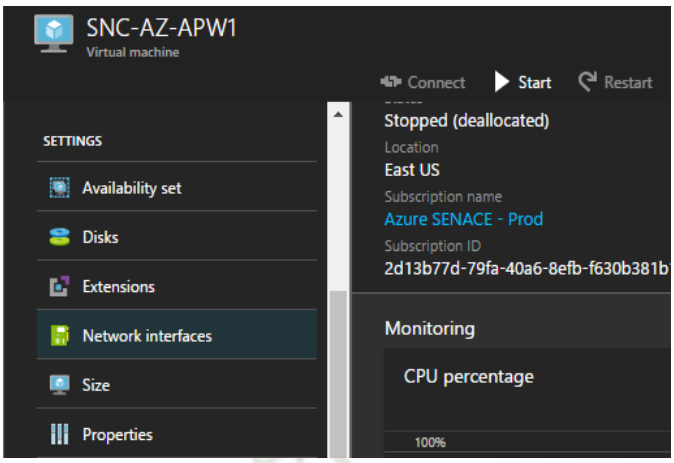
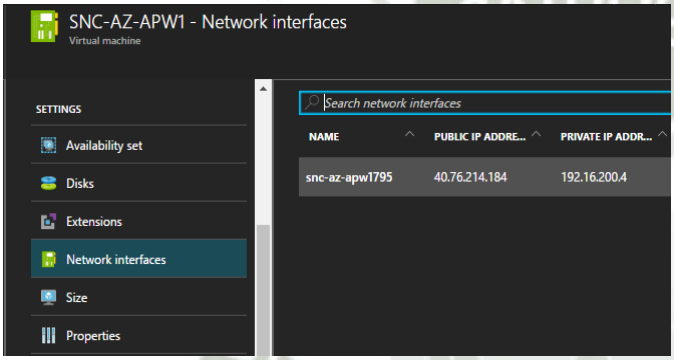
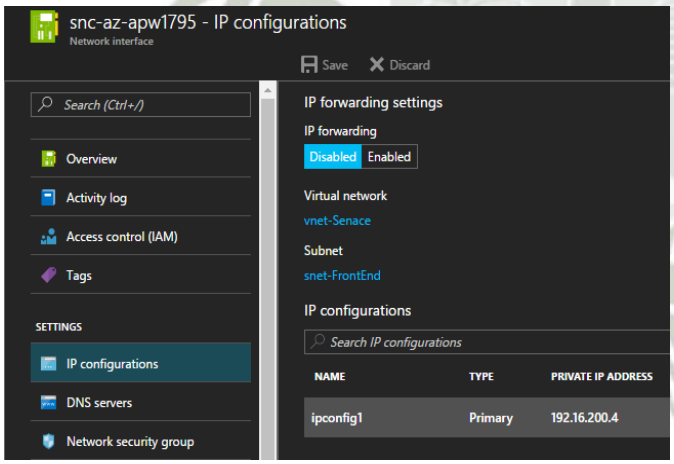
Ventana	Acción
	Seleccionar **Attach new** y completar los siguientes campos: • **Name:** SNC-AZ-BD2-disk1 • **Type:** HDD • **Size:** 200 • **Host caching:** None Seleccionar **OK**
	Al finalizar, visualizamos el disco de datos creado.

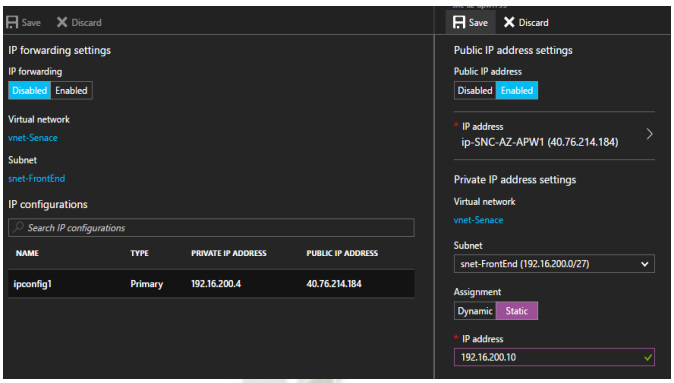
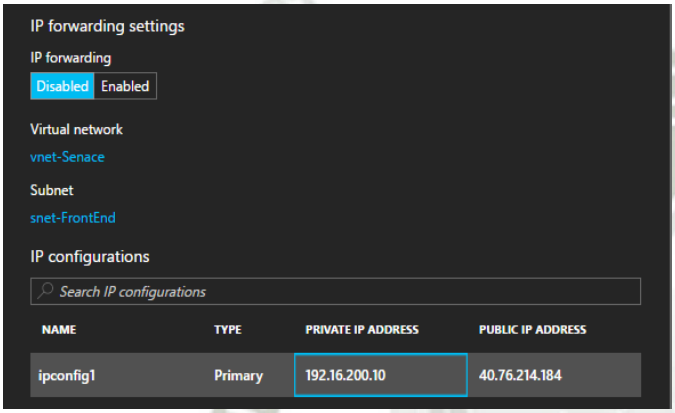
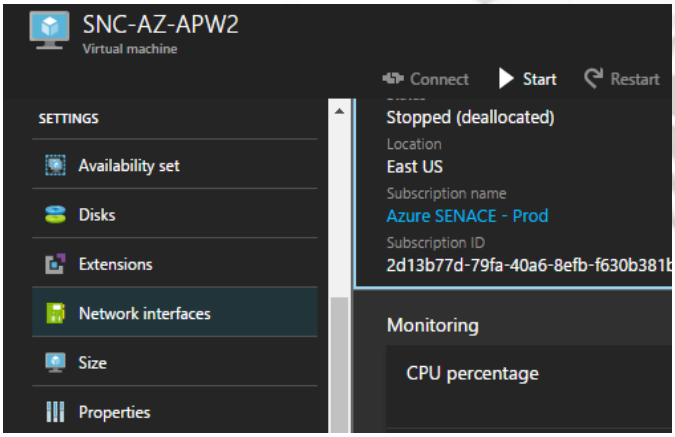
Fuente: Elaboración Propia

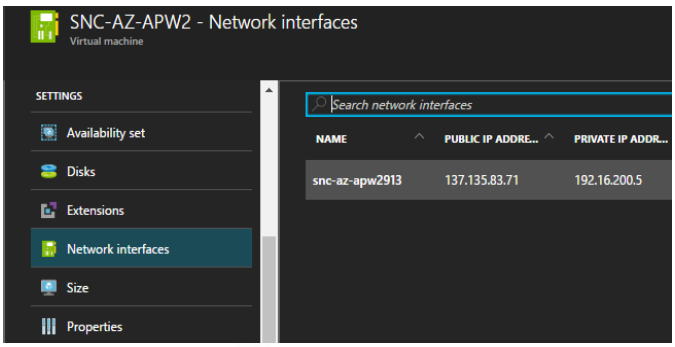
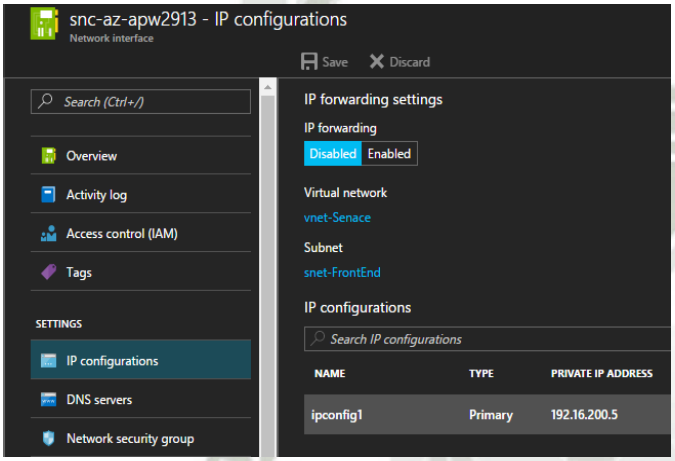
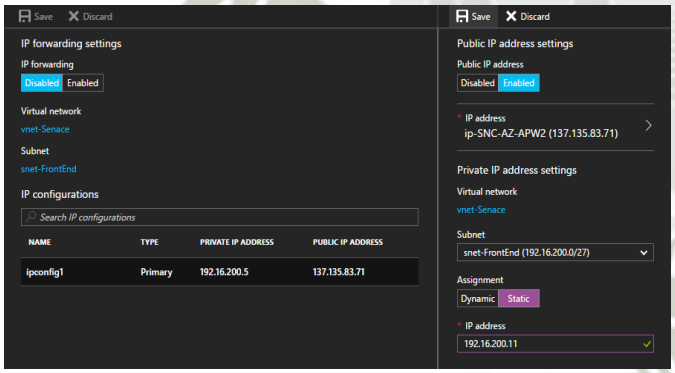
1.5.8 IP Privade

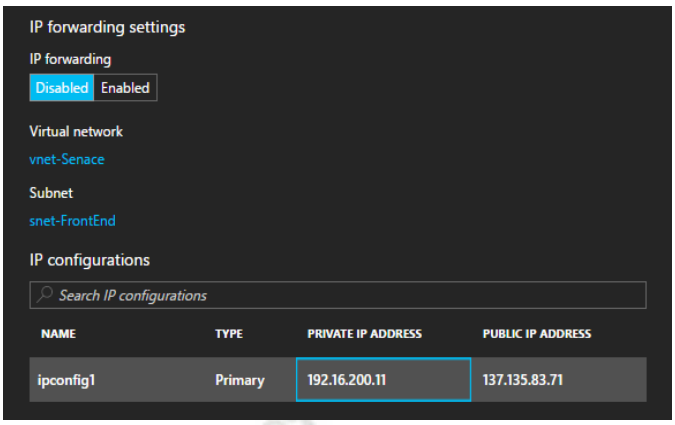
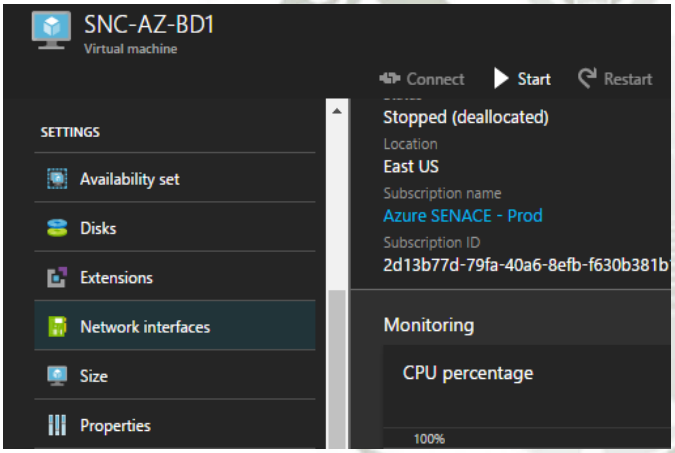
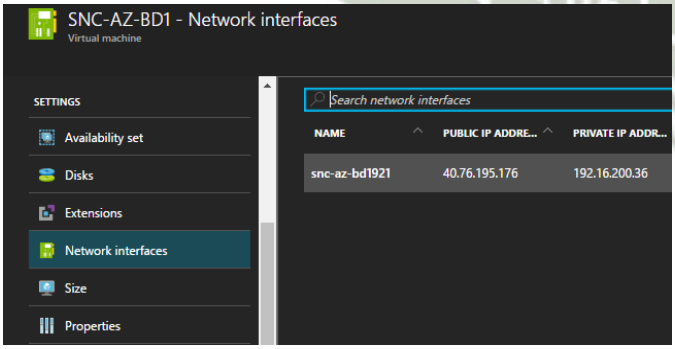
Tabla 7: Creación de IP Private

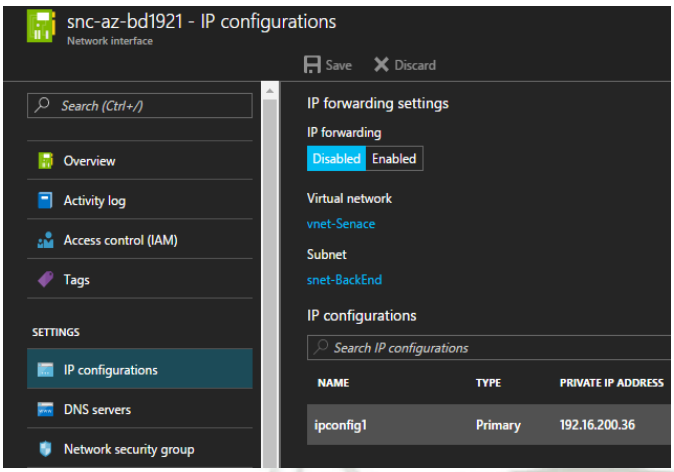
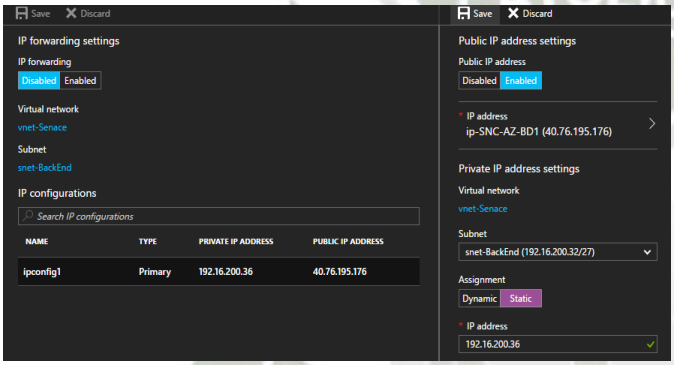
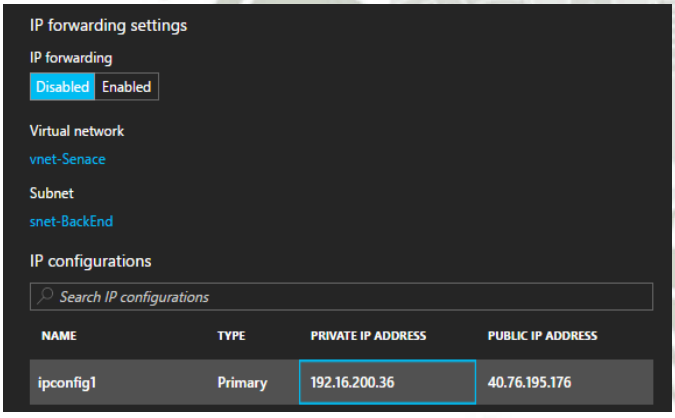
Ventana	Acción
	Se procederá a realizar la configuración de las **Network Interfaces** para cada máquina virtual.

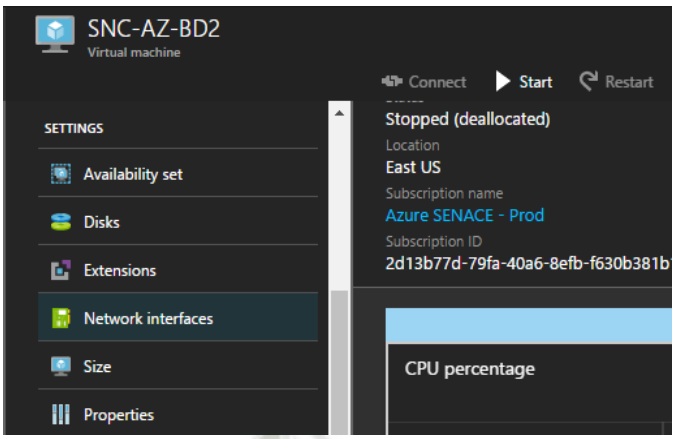
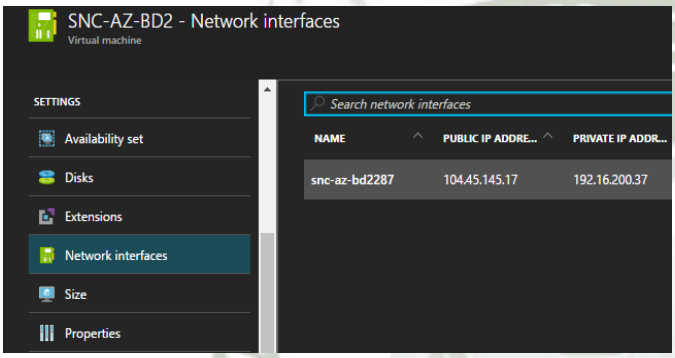
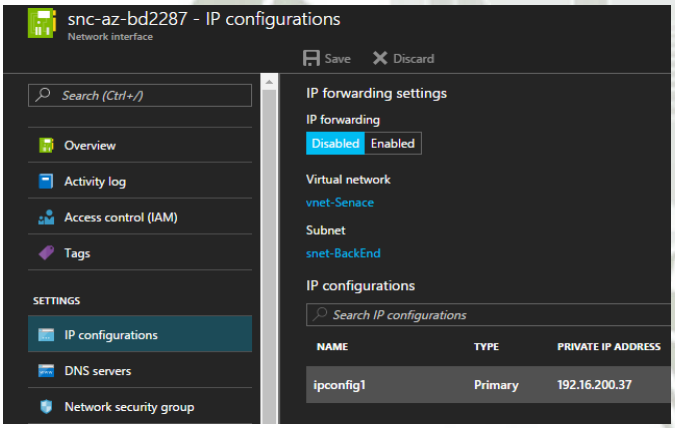
Ventana	Acción
	Seleccionar **Virtual machine > SNC-AZ-APW1 > Network interfaces**.
	Seleccionar **snc-az-apw1795.**
	Seleccionar **IP configurations > ipconfig1**

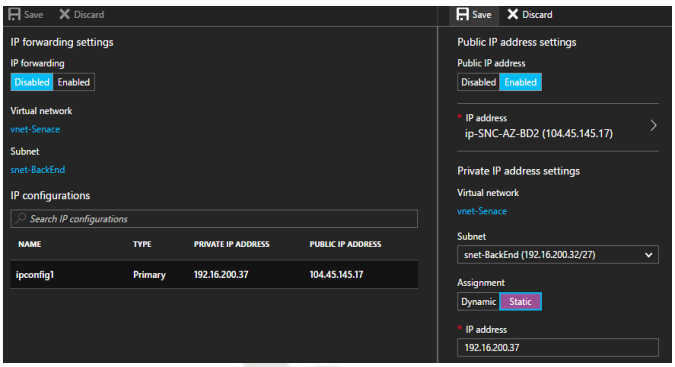
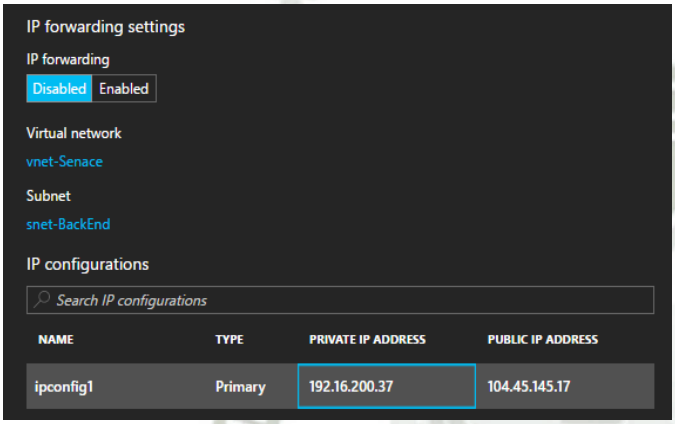
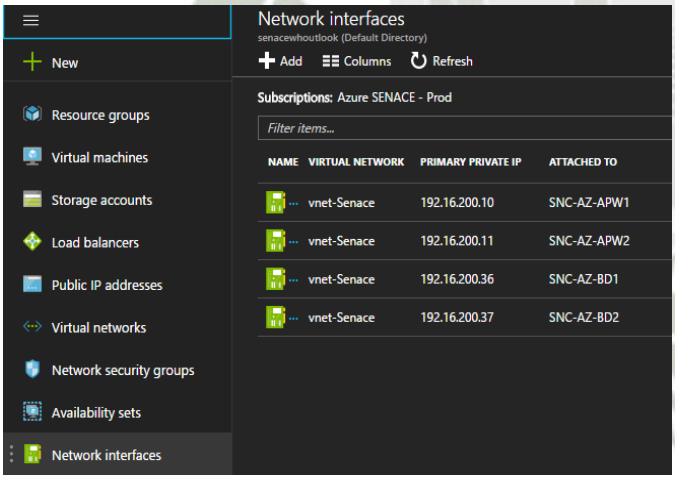
Ventana	Acción
	Seleccionar **Assigment Static** en la sección **Private IP address settings** e ingresar la ip correspondiente del servidor. Seleccionar **Save**.
	Al finalizar en la sección **IP configurations**, se visualiza la ip privada configurada.
	Se procederá a realizar la configuración de la **Network Interfaces** para la máquina virtual **SNC-AZ-APW2**
	Seleccionar **Virtual machine** > **SNC-AZ-APW2** > **Network interfaces**.

Ventana	Acción
	Seleccionar **snc-az-apw2913.**
	Seleccionar **IP configurations** > **ipconfig1**
	Seleccionar **Assigment Static** en la sección **Private IP address settings** e ingresar la ip correspondiente del servidor. Seleccionar **Save**.

Ventana	Acción
	Al finalizar en la sección **IP configurations**, se visualiza la ip privada configurada.
	Se procederá a realizar la configuración de la **Network Interfaces** para la máquina virtual **VM-BD1.**
	Seleccionar **Virtual machine > SNC-AZ-BD1 > Network interfaces**.
	Seleccionar **snc-az-bd1921**.

Ventana	Acción
	Seleccionar **IP configurations** > **ipconfig1**
	Seleccionar **Assigment Static** en la sección **Private IP address settings** e ingresar la ip correspondiente del servidor. Seleccionar **Save**.
	Al finalizar en la sección **IP configurations**, se visualiza la ip privada configurada.
	Se procederá a realizar la configuración de la **Network Interfaces** para la máquina virtual **VM-BD2**

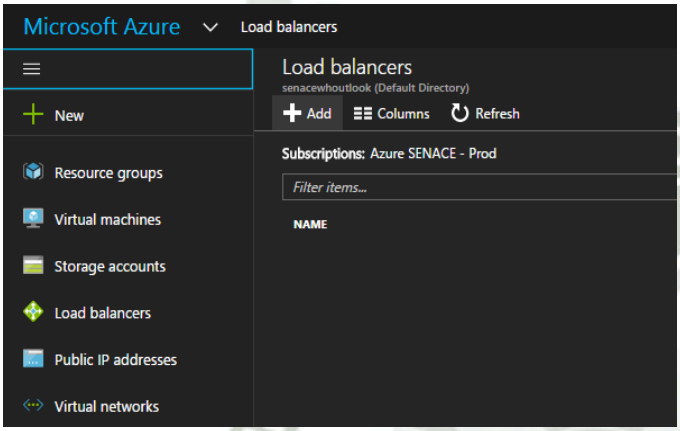
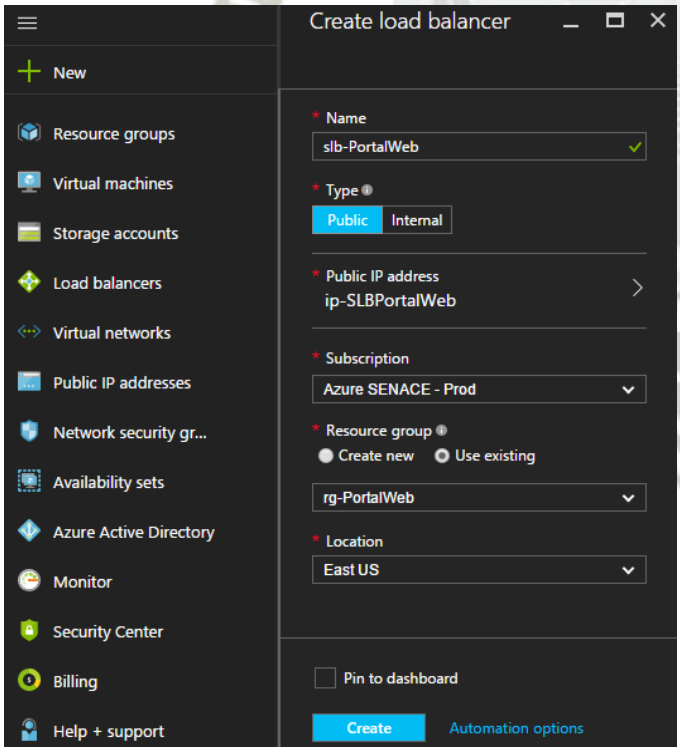
Ventana	Acción
	Seleccionar **Virtual machine > SNC-AZ-BD2 > Network interfaces**.
	Seleccionar **snc-az-bd2287**.
	Seleccionar **IP configurations > ipconfig1**

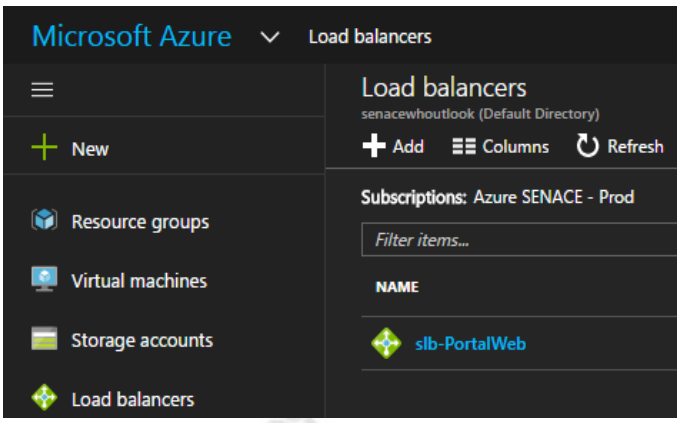
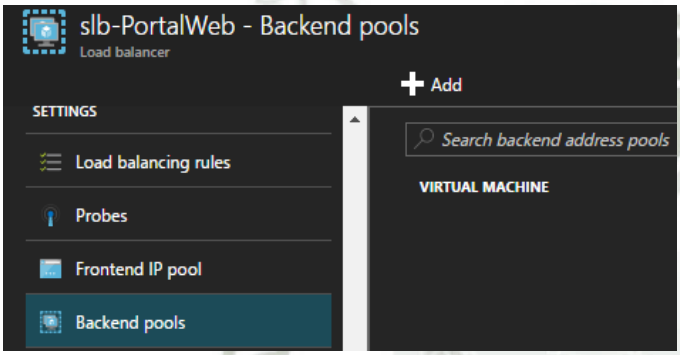
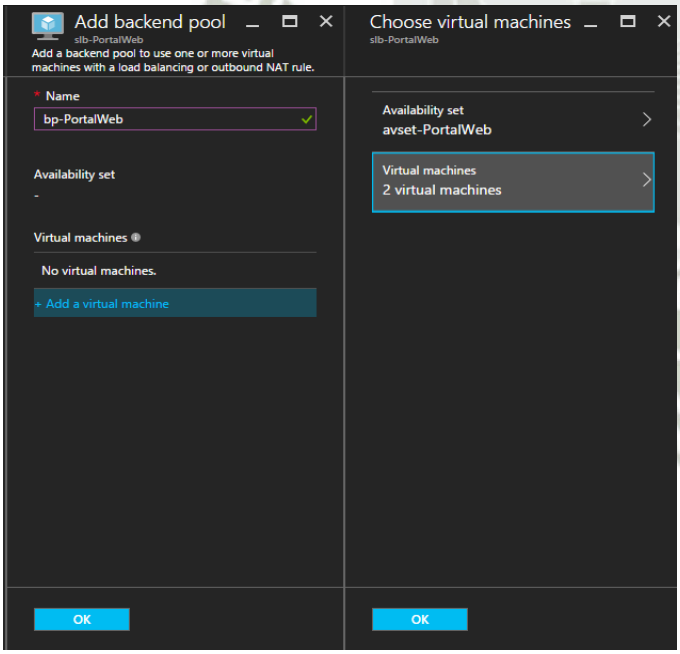
Ventana	Acción
	Seleccionar **Assigment Static** en la sección **Private IP address settings** e ingresar la ip correspondiente del servidor. Seleccionar **Save**.
	Al finalizar en la sección **IP configurations**, se visualiza la ip privada configurada.
	Al finalizar, visualizamos las **Networks interfaces** creadas.

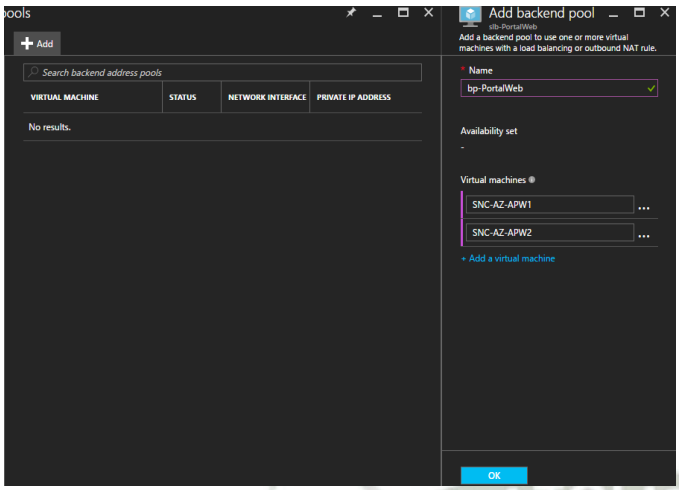
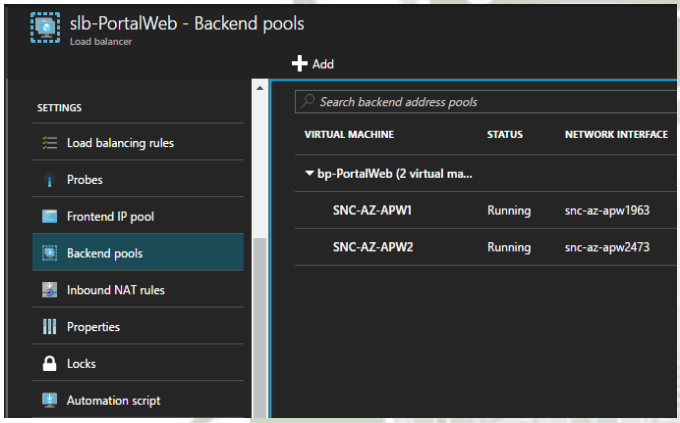
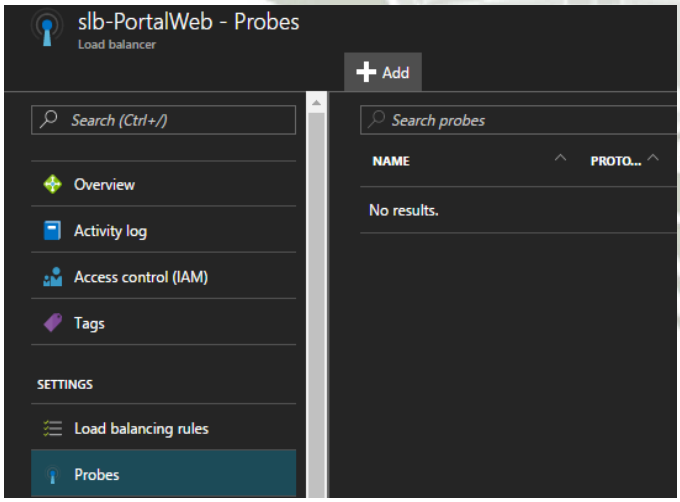
Fuente: Elaboración Propia

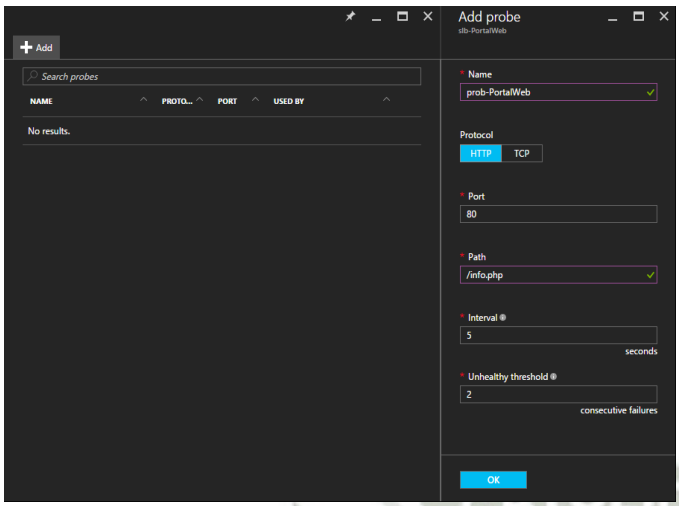
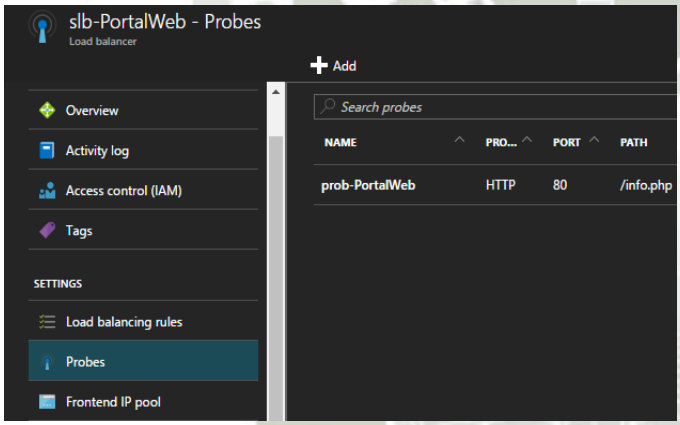
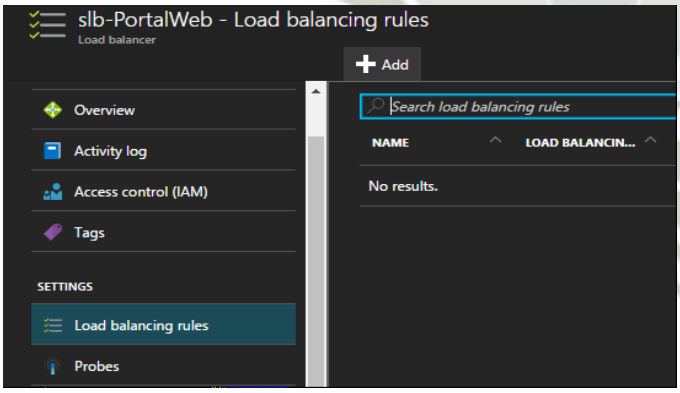
1.5.9 External Load Balancer

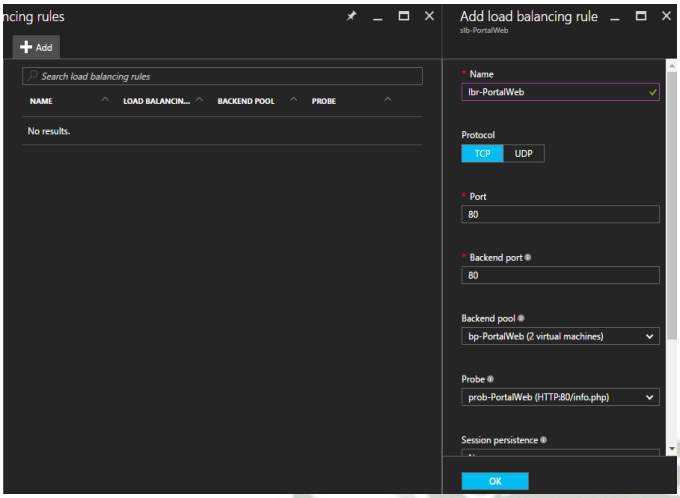
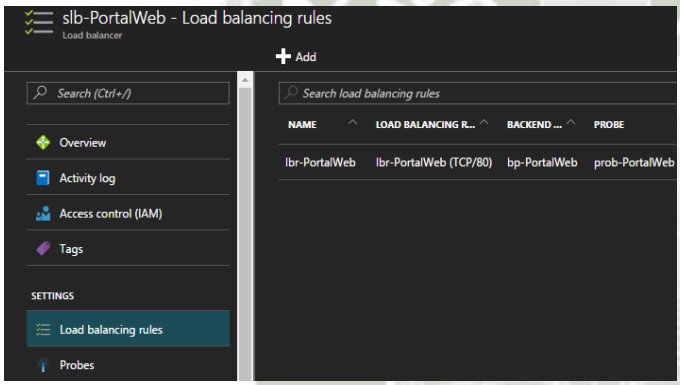
Tabla 08: Creación y configuración de External Load Balancer

Ventana	Acción
	Se procederá a realizar la creación del **ExternalLoad Balancer** para balancear la carga del Portal Web.
	Seleccionar **Load Balancer** > **Add**
	Para la creación del **balanceador web,** completar los siguientes campos: • **Name:** slb-PortalWeb • **Public IP address:** ip-SLBPortalWeb • **Subscription:** Azure SENACE - Prod • **Resource group:** rg-PortalWeb • **Location:** East US Seleccionar **Create.**

Ventana	Acción
	Al finalizar, visualizamos el **Load balancer** creado.
	Seleccionar **slb-PortalWeb** > **Backend pools** > **Add**.
	En la sección **Add backend pool**, ingresar los siguientes campos: • **Name:** bp-PortalWeb • **Availability Set:** avset-PortalWeb • **Virtual Machine:** SNZ-AZ-APW1 SNZ-AZ-APW2 Seleccionar **OK.**

Ventana	Acción
	Seleccionar **OK.**
	Al finalizar, el **backend pool** deberá mostrar las máquinas virtuales seleccionadas.
	Seleccionar **Probes > Add**

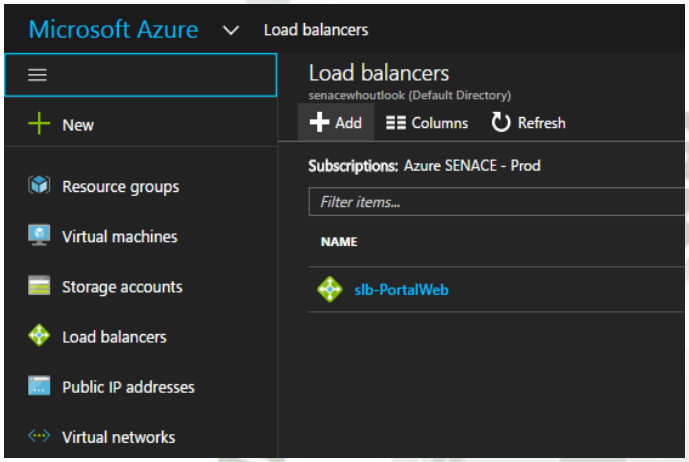
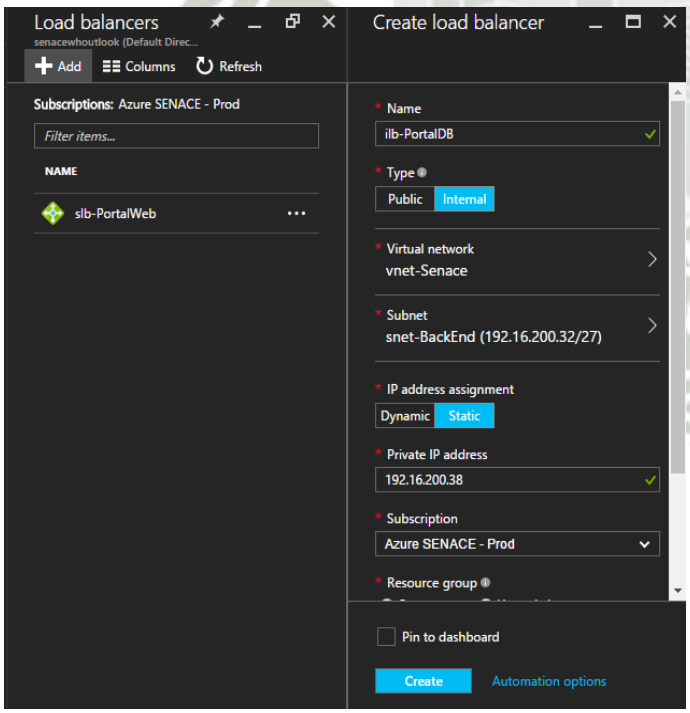
Ventana	Acción
	En la sección **Add probe,** ingresar los siguientes campos: • **Name:** prob-PortalWeb • **Protocol:** HTTP • **Port:** 80 • **Path:** /Info.php • **Interval:** 5 • **U threshold:** 2 Seleccionar **OK**.
	Al finalizar, se visualiza los **Probes** creados.
	Seleccionar **Load balancing** > **Add**

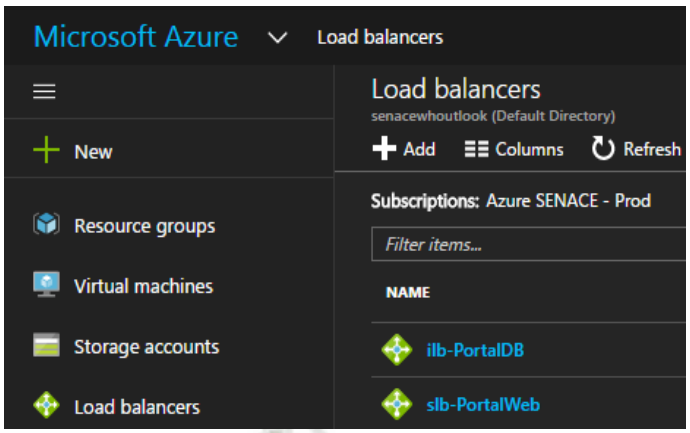
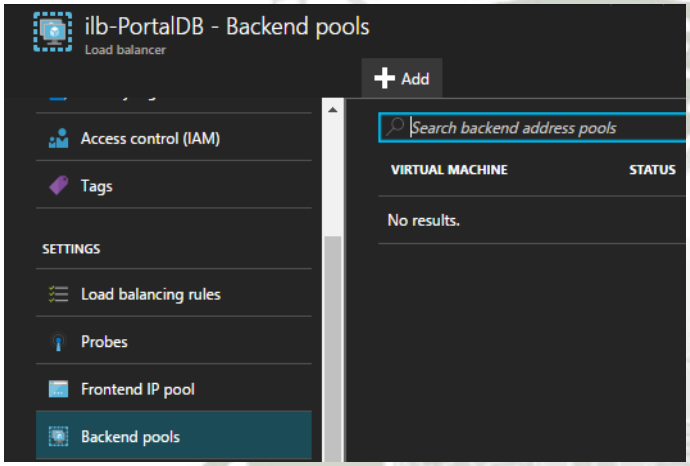
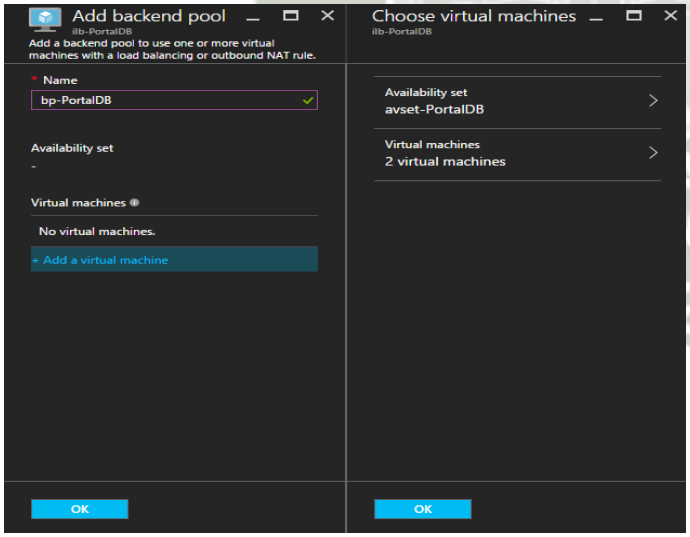
Ventana	Acción
	En la sección **Add load balancing rule**, completar los siguientes campos: • **Name:** lbr-PortalWeb • **Protocol:** TCP • **Port:** 80 • **Backend port:** 80 • **Backend pool:** bp-PortalWeb • **Probe:** prob-PortalWeb Seleccionar **OK**
	Al finalizar, se visualiza el **Load balancing rules** creado.

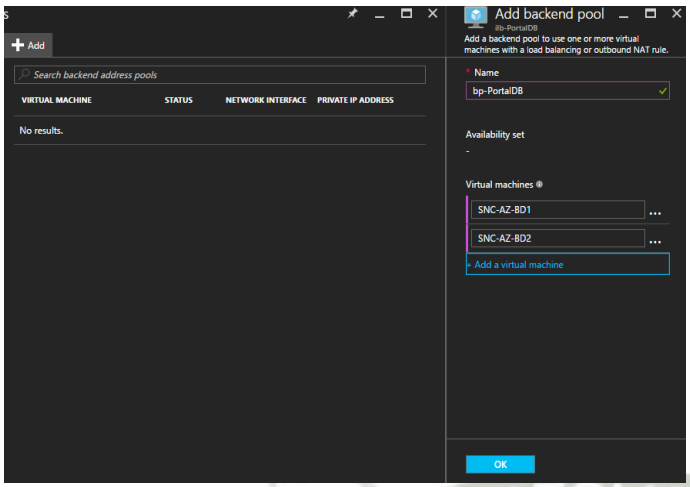
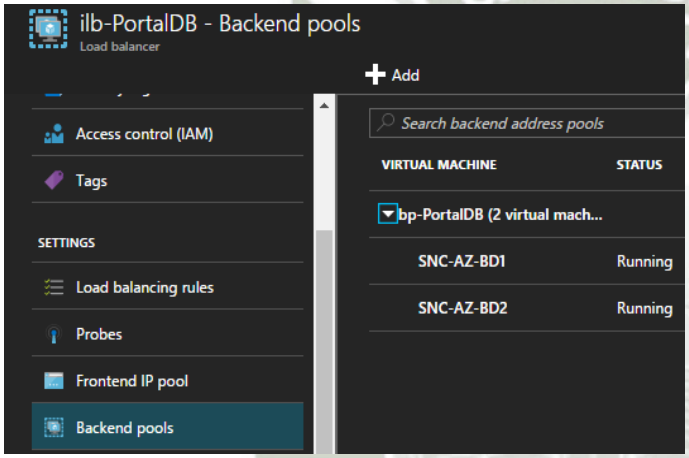
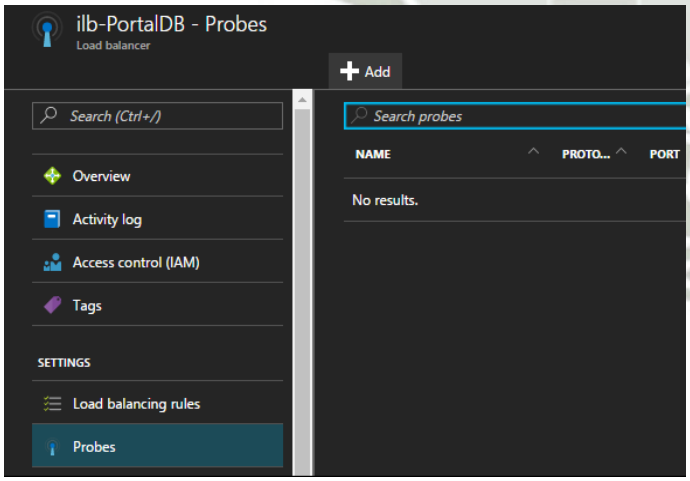
Fuente: Elaboración Propia

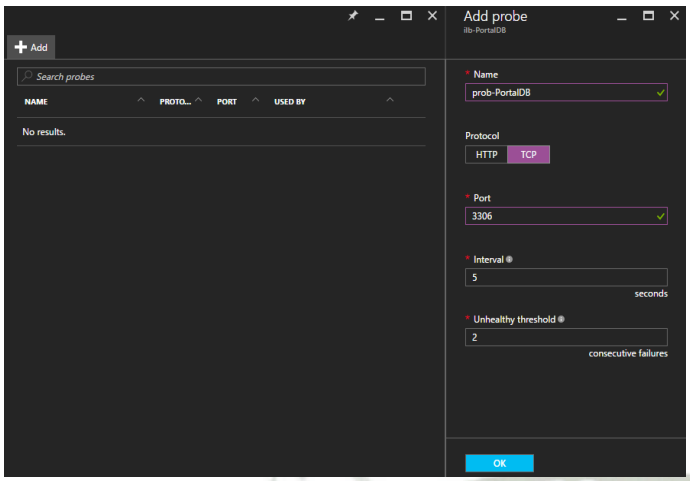
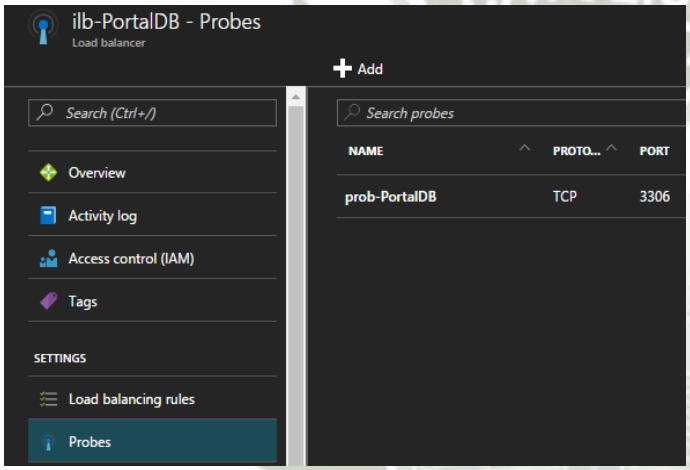
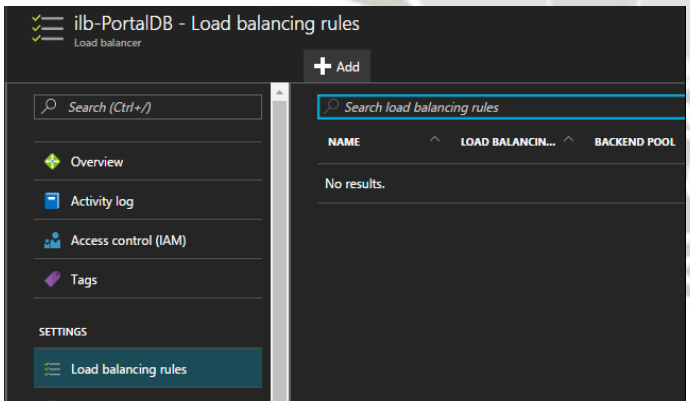
1.5.10 Internal Load Balancer

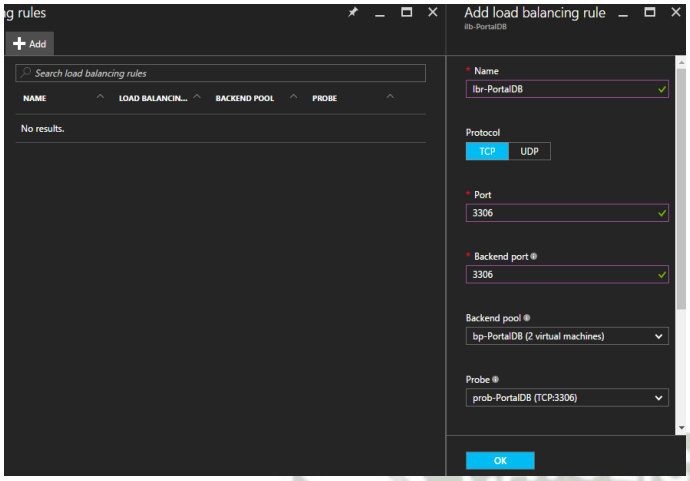
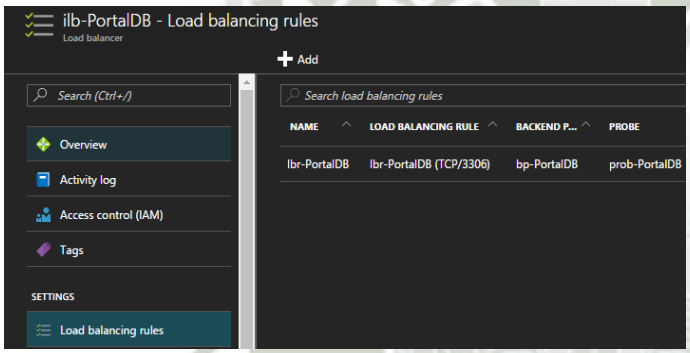
Tabla 09: Creación y configuración de Public Load Balancer

Ventana	Acción
	Se procederá a realizar la creación del **InternalLoad Balancer** para balancear la carga de base de datos.
	Seleccionar **Load balancers > Add.**
	En la sección **Create load balancer,** completar los siguientes campos**:** • **Name:** ilb-PortalDB • **Type:** Internal • **Virtual Network:** vnet-Senace • **Subnet:** snet-BackEnd • **Subscription:** Azure SENACE - Prod • **Resource group:** rg-PortalWeb • **Location:** East US Seleccionar **Create.**

Ventana	Acción
	Al finalizar, visualizamos el **Load balancer** creado.
	Seleccionar **Backend pools > Add**
	En la sección **Add backend pool**, ingresar los siguientes campos: • **Name:** bp-PortalDB • **Availability Set:** avset-PortalDB • **Virtual Machine:** SNZ-AZ-DB1;SNZ-AZ-DB2 Seleccionar **OK.**

Ventana	Acción
	Seleccionar **OK.**
	Al finalizar, el **backend pool** deberá mostrar las máquinas virtuales seleccionadas.
	Seleccionar **Probes** > **Add**

Ventana	Acción
	En la sección **Add probe,** ingresar los siguientes campos: • **Name:** prob-PortalDB • **Protocol:** TCP • **Port:** 3306 • **Interval:** 5 • **U threshold:** 2 Seleccionar **OK**.
	Al finalizar, se visualiza el **Probes** creado.
	Seleccionar **Load balancing rules** > **Add**

Ventana	Acción
	En la sección **Add load balancing rule**, completar los siguientes campos: • **Name:** lbr-PortalDB • **Protocol:** TCP • **Port:** 3306 • **Backend port:** 3306 • **Backend pool:** bp-PortalDB • **Probe:** prob-PortalDB • Seleccionar **OK**
	Al finalizar, se visualiza el **Load balancing rules** creado.

Fuente: Elaboración Propia

Capítulo 2: Documentación Técnica

2.1. Plan del Proyecto Informático

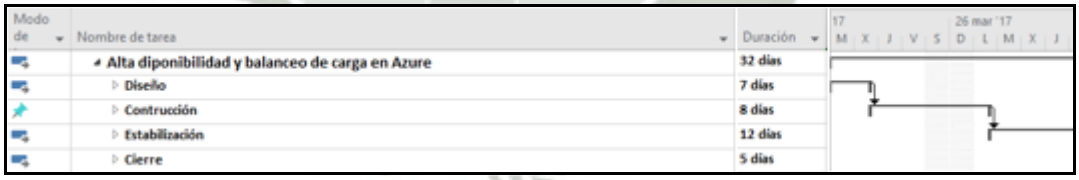
2.1.1. Planificación del Proyecto

Para la realización del proyecto en desarrollo se realizó un diagrama de Gantt en el cuál se podrá identificar las tareas para realizar y las fechas en las cuales se realizarán cada una de estas, cada tarea cuenta con sub tareas para realizar a continuación se determinarán los principales procesos del proyecto en desarrollo.

- Diseño
- Construcción
- Estabilización
- Cierre

Dichas tareas serán mostradas en el siguiente diagrama de Gantt, además de la secuencia en la que se realizó cada proceso (Figura 8). También se determina la duración de cada proceso según el número de dedicación efectiva indicada en horas/hombre.

Figura 8: Diagrama de Gantt de los procesos de proyecto

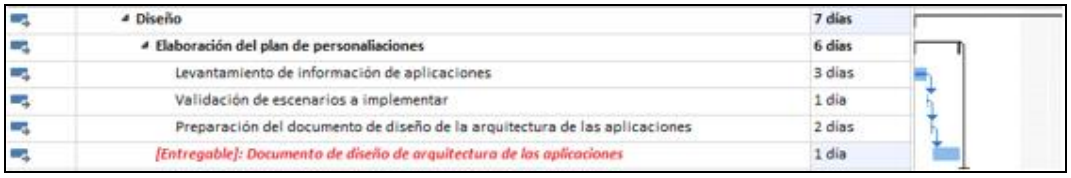


Fuente: Elaboración propia

A continuación, se muestra el plan de actividades de cada uno de los procesos determinados para el proyecto, para empezar, se muestra el plan de actividades de la fase de diseño, en la cual se detallan las subtareas, además se indica el tiempo de

duración de cada una de estas y la secuencia que cada una debe seguir (Figura 9). Con lo que se logra determinar que la fase de diseño será de una duración de 7 días.

Figura 9: Diagrama de Gantt de la fase de Diseño



Fuente: Elaboración propia

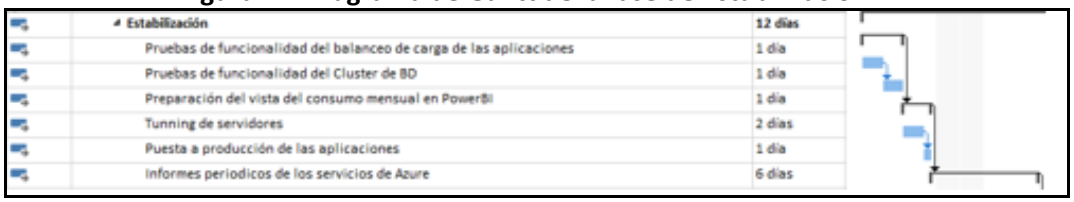
Posteriormente se realizó el planeamiento de la fase de construcción, en la cual se propuso un subproceso principal, la elaboración del plan de personalidades, cuya importancia está basada en la recolección de información del estado situacional de la empresa y sus requerimientos (Figura 10). Se determinó las tareas de cada uno de este subproceso, además se asignan las fechas de inicio y fin, por lo que se determina que el desarrollo de sistema tendrá una duración de 8 días de trabajo.

Figura 10: Diagrama de Gantt de la fase de Construcción

Fuente: Elaboración propia

Después de la fase de estabilización, se desarrolla la planeación del cronograma de la fase de pruebas, en la que se encontraron subtareas y se asignan las fechas necesarias para este proceso (Figura 11). Se determinó que la fase de pruebas del proyecto tendrá una duración de 2 semanas.

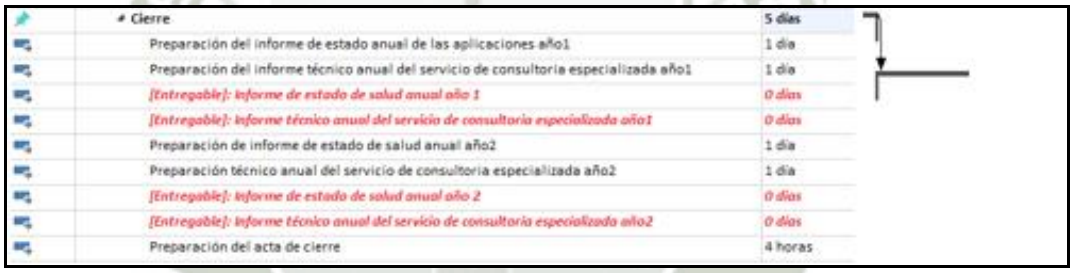
Figura 11: Diagrama de Gantt de la fase de Estabilización



Fuente: Elaboración propia

Posteriormente se determinó el cronograma para la fase de cierre, se identificaron las sub tareas que tiene este proceso y se indicó los 32 días de duración de cada una de estas y las fechas en la que se desarrollaron (Figura 12). Cabe recalcar que la fase de cierre incluye los resultados y entregables del proyecto y tendrá una duración de 5 días.

Figura 12: Diagrama de Gantt de la fase Cierre



Fuente: Elaboración propia

2.1.2. Estudio de Viabilidad del Proyecto

2.1.2.1. Descripción de Productos y Servicios

Se consideró indispensable contar con la plataforma informática Azure ya que, se requiere un escenario en alta disponibilidad para la migración a la nube de los servicios alojados localmente en la institución.

El diseño de la arquitectura contempla almacenamiento, transferencia de datos, balanceo de carga interna y externa, grupos de seguridad y disponibilidad establecida.

Se consideró también un entorno gráfico para el monitoreo de consumo por componentes en la infraestructura y costo de los mismo, contemplando el procesamiento de datos para la toma de decisiones.

2.1.2.2. Consideraciones Tecnológicas

- Las capacidades del servicio de cloud hosting a nivel de aplicación permiten múltiples lenguajes de programación como: PHP, Java, .NETcomo mínimo.
- El servicio de cloud hosting deberá utilizar MySQL 5.5 de 64 bits como motor de base de datos.
- Los cambios en la configuración de la infraestructura del servicio han sido y serán coordinados con la institución.
- Los servicios alojados son respaldados periódicamente en base a los requerimientos y necesidades de la entidad.
- Para la solución de cloud hosting de la institución se gestionó la asignación de recursos de capacidad de cómputo con la finalidad de garantizar el desarrollo de los servicios indicados.
- El servicio permite el balanceo de carga de trabajo y distribuir un tipo específico de tráfico proveniente de internet entre los servidores de la solución, considerando que la aplicación soporta un escenario de alta disponibilidad, el cual ha sido configurado e implementado.
- Se asegura que el servicio de cloud hosting es robusto y estable frente a ataques de denegación de servicio.

2.1.2.3. Características del Producto

ID	Componentes Mínimos de la solución	Cantidad(*)	Tipo
1	Máquinas Virtuales (4 x 1.6 GHz CPU, 7GB RAM)	4	VM
2	Transferencia de datos	500	GB

2.1.2.4. Estrategia de Marketing

2.1.2.4.1. Alta Disponibilidad

El contexto de alta disponibilidad hace referencia a la capacidad de despliegue que tiene la nube para seguir proveyendo los servicios que contenga la implementación desplegada, aun cuando existan situaciones planeadas o no que afecten al hardware, al sistema operativo, a las comunicaciones.

2.1.2.4.2. Seguridad

Microsoft ha aprovechado décadas de experiencia en la compilación de software empresarial y en la ejecución de algunos de los mayores servicios en línea del mundo para crear un conjunto sólido de tecnologías y prácticas de seguridad. Estas últimas aseguran que la infraestructura de Azure sea resistente a los ataques, salvaguarda el acceso de los usuarios al entorno de Azure y protege los datos de los clientes mediante comunicaciones cifradas, así como la administración de amenazas y prácticas de mitigación, incluidas pruebas de penetración regulares.

2.1.2.4.3. Redundancia

Los mayores servicios informáticos en la nube se ejecutan en una red mundial de centros de datos seguros, que se actualizan periódicamente con el hardware más rápido y eficiente de última generación. Esto aporta varias ventajas en comparación con un

único centro de datos corporativo, entre las que se incluyen una latencia de red menor para las aplicaciones y mayores economías de escala.

2.1.2.4.4. Escalabilidad

La facilidad y rapidez para el incremento de hardware en un momento de alta demanda es imprescindible para las publicaciones de nuevos aplicativos y servicios a través de Internet por las diferentes empresas.

2.1.2.4.5. Análisis de datos

A medida que se generan más cantidad de datos desde los diferentes componentes implementados, la transformación de estos datos en predicciones y perspectivas útiles casi en tiempo real ahora resulta una necesidad operativa.

2.1.2.4.6. Costos Reducidos

La informática y el almacenamiento se transforman en una base a petición que puede usar en cualquier momento, pagando sólo lo que realmente usa. Con la computación en nube, un modelo de costos reemplaza a ese modelo de inversión. Se paga por recursos, como la potencia del servidor y el almacenamiento en base a su uso real.

2.1.2.5. Organización y Recursos Humanos

- ✓ Arquitecto de soluciones en tecnologías del modelo del servicio de cloud computing (Microsoft Azure).
- ✓ Consultor Especialista en soluciones Cloud Computing.

2.1.2.6. Proyecciones Financieras

Se ofrece a la entidad un contrato del tipo Enterprise cuya ventaja principal son precios inmejorables ya que Microsoft continúa ofreciendo innovaciones de Azure al mercado mejorando la transparencia y simplicidad, todo esto para garantizar que se encuentre un precio muy bueno considerando que con el tipo de contratación Enterprice siempre son más bajos que los AWS de Azure.com para servicios comparables.

Los pagos son anuales, respecto al saldo solicitado por la entidad, enfocado en sus necesidades y crecimiento, teniendo en cuenta que el costo en Azure es solo por uso.

2.2. Especificación de Requisitos de Software

- El servicio de Cloud Hosting soportará la siguiente plataforma tecnológica: PHP 7 o última versión estable con librerías GDLIB v.2.034 con freetype.
- El servicio de Cloud Hosting tiene habilitado las extensiones: pdo_mysql, mcrypto, pdo_ocl.
- El portal web institucional está desarrollado en la plataforma de WordPress 4.5.3.
- La arquitectura tecnológica de los servidores implementados en el servicio de Cloud Hosting es de 64 bits.
- El sistema operativo distribuido será Windows Server 2012 R2.
- La plataforma de cloud hosting propuesta, permite el correcto funcionamiento y rendimiento de las aplicaciones a soportar.
- El servidor web va a soportar las versiones de Apache HTTP 2.4.7 o la última versión estable.

- El diseño de la arquitectura de los componentes de la plataforma en modelos IaaS en donde las aplicaciones son instaladas.

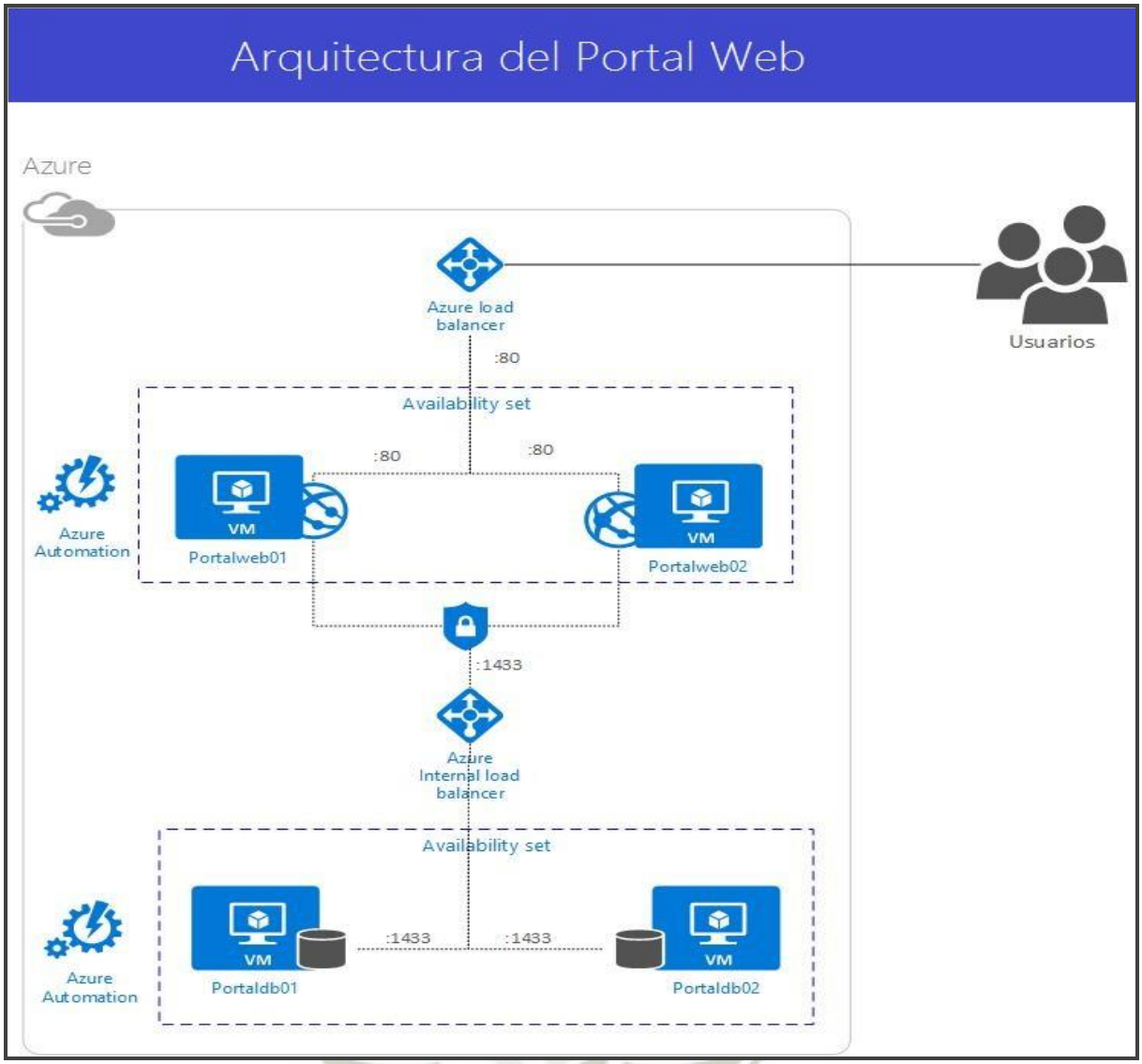
2.3. Especificación de Diseño

Los componentes de la solución de gestión de servicios y/o aplicaciones son máquinas virtuales (IaaS), Cloud Services, Storage Account y Virtual Network. De manera específica, Microsoft Azure es líder en Cloud Computing debido a sus diversos servicios, uso intuitivo y seguridad de información (Figura 13).

Después de un análisis y evaluación sobre los requerimientos para el inicio del proyecto, se consideró implementar una solución que le permita gestionar de manera más óptima los recursos de la compañía, minimizar costos y asegurar la continuidad de su aplicación web.

Su portal web y aplicaciones ligadas son soportados sobre tecnología Microsoft, donde se implementó la infraestructura diseñada a continuación presentada.

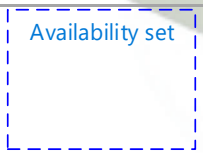
Figura 13: Arquitectura del Servicio Portal Web



Fuente: Elaboración Propia

2.3.1. Descripción de Componentes:

Tabla 10: Componentes del servicio Portal Web

Componente	Descripción del componente
	**Resource Group,** es un componente que tiene almacenados recursos relacionados de una aplicación.
	**Azure Load balancer**, es un componente de balanceo de carga externo. Para el portal institucional se usará para la distribución equilibrada del puerto: 80 en los servidores web.
	**Azure Load Internal Balancer**, es un componente de balanceo de carga interno. Para el portal institucional se usará para la distribución equilibrada de base de datos, la cual estará configurada en un clúster de base de datos Activo – Activo.
	**Availability Set**, es un componente que permite a las máquinas virtuales obtener un SLA mensual del 99,95%. Esto solo se cumple si las máquinas virtuales tienen un Fault Domain y Update Domain distintos. Cabe resaltar que ambas maquinas deben tener el mismo rol.
	**Network Security Group**, es un componente que nos permitirá configurar la seguridad de nuestras redes.

 Virtual machine	**Virtual Machine**, es una máquina virtual que alojará los servicios de base de datos y aplicativo web.
 Azure Automation	**Azure Automation**, es un componente que permitirá automatizar las máquinas virtuales cuando el consumo de hardware sea bajo.

Fuente: Elaboración Propia

2.4. Documentación Técnica

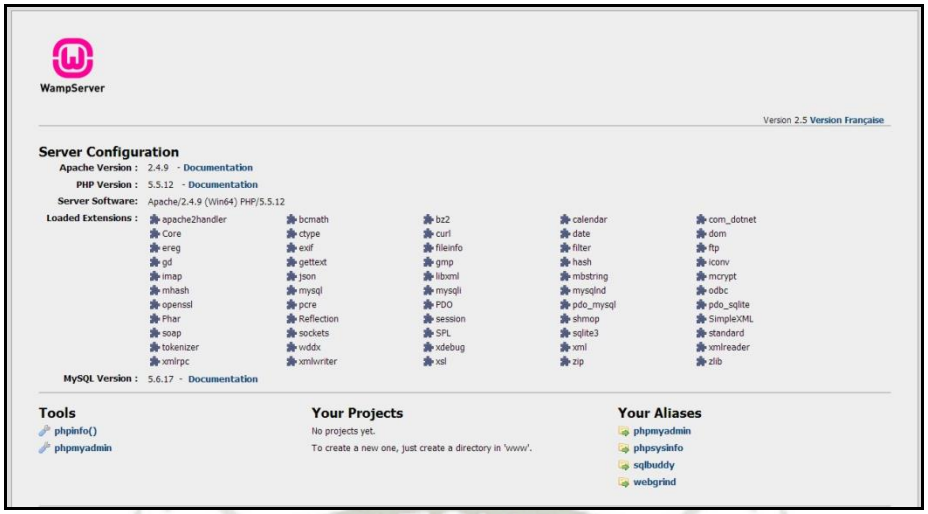
2.4.1. Lenguajes y Herramientas

2.4.1.1. WampServer

WampServer es un entorno de desarrollo web para el sistema operativo Windows que trabaja con Apache, PHP, y como motor de base de datos PHPMyadmin (Figura 14), este entorno es utilizado en sus servidores locales para que contengan la plataforma semántica WordPress y su respectiva base de datos Mysql.

Todas las características y configuraciones son replicadas en los servidores implementados, para que, al momento de la migración, sea un proceso transparente y no haya problemas de compatibilidad.

Figura 14: Plataforma Wamp



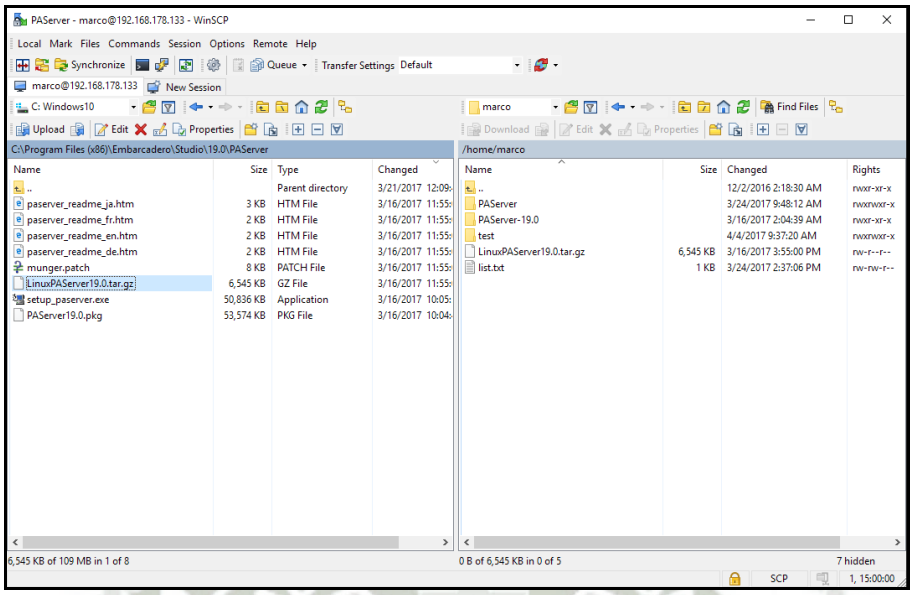
Fuente: Elaboración Propia

2.4.1.2. WinSCP

Es un cliente SFTP grafico para el sistema operativo Windows que utiliza el protocolo SSH, esta herramienta tiene como objetivo principal la transferencia de datos entre servidores de manera segura, esta herramienta se instaló en uno de los servidores implementados en Azure (Figura 15), para la replicación de las fuentes del aplicativo Portal Web, ya que los servidores de capa web son dos, como se especificó en el diseño.

La ventaja de esta herramienta instalada en un servidor alojado en la nube, es que la transferencia no puede ser interrumpida ya que todo el tráfico es virtual.

Figura 15: Entorno gráfico WinSCP



Fuente: Elaboración Propia

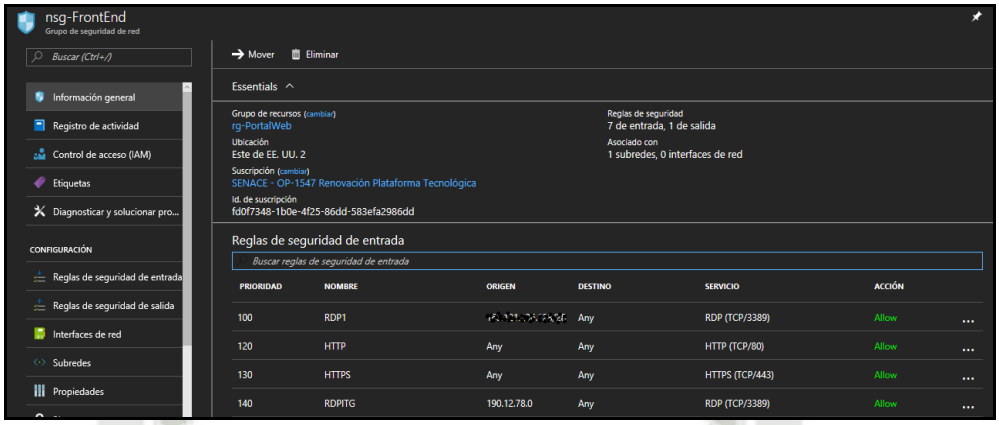
2.4.2. Control de Acceso

Con el fin de sostener una administración y control de accesos, se procedió a crear un grupo de seguridad de red o también simplificado (NSG) que contiene una lista de reglas de seguridad que permiten o deniegan el tráfico de red a recursos conectados a redes virtuales de Azure (VNet).

Los grupos de seguridad de red pueden ser asociados a subredes, interfaces de red y máquinas virtuales individuales (Figura 16). Cuando un grupo de seguridad de red está asociado a una subred, las reglas van a ser aplicadas a todos los recursos que se encuentren conectados a la subred.

El tráfico se puede restringir aún más si se asocia también un grupo de seguridad de red a una máquina virtual de manera individual o interfaz de red.

Figura 16: Reglas de control de accesos



Fuente: *Elaboración Propia*

2.5. Pruebas de Ejecución

2.5.1. Pruebas de Seguridad

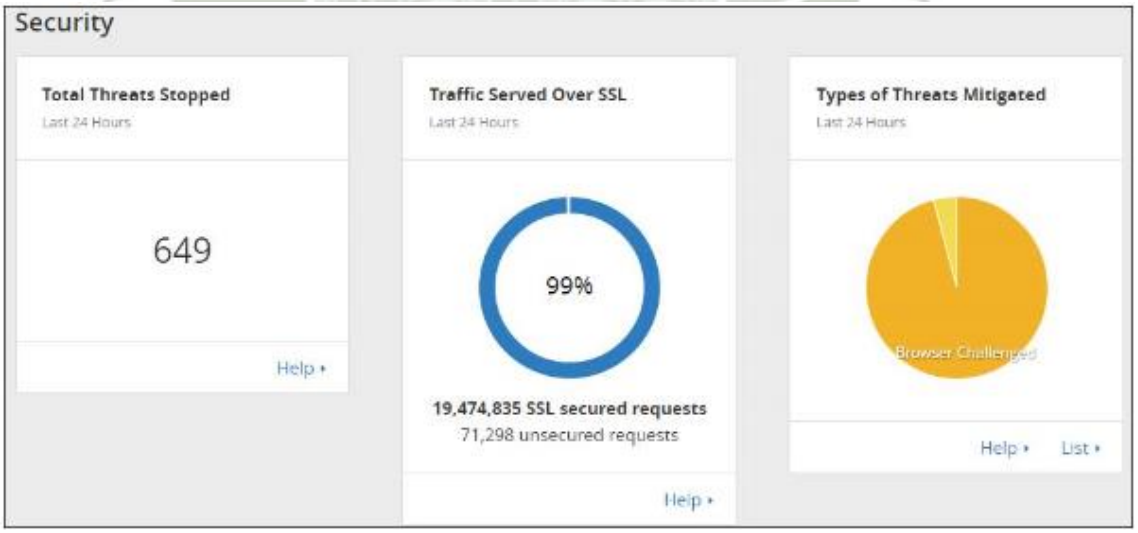
El CDN Clouflare tiene como objetivo guardar de manera temporal el contenido estatico del servicio publicado, esto para que el servidor tenga menos peticiones directas y a la vez haya un análisis de estas al trabajar como un proxy (Figura 17).

En el entorno gráfico, podemos observar la cantidad de solicitudes y los posibles intentos maliciosos que ponen en peligro la disponibilidad e integridad de la información, dando tiempo suficiente para accionar y bloquear a posibles intrusos (Figura 18).

Figura 17: Gráfico de Incidentes

Fuente: Resultados Cludflare

Figura 18: Gráficas del Detalle del Tráfico



Fuente: Resultados Cloudflare

Descripción de los tipos de amenazas en los que se divide las alertas de Cloudflare (Figura 19).

1. Desafío del navegador:

Un bot no responde a un desafío de JavaScript. Durante un desafío de JavaScript se mostrará una página intermedia durante unos cinco segundos mientras Cloudflare realiza una serie de desafíos matemáticos para asegurarse de que es un visitante humano legítimo.

2. Mala navegación:

La fuente de la solicitud no era legítima o la solicitud en sí era maliciosa. El usuario vería una página de error 1010 en su navegador.

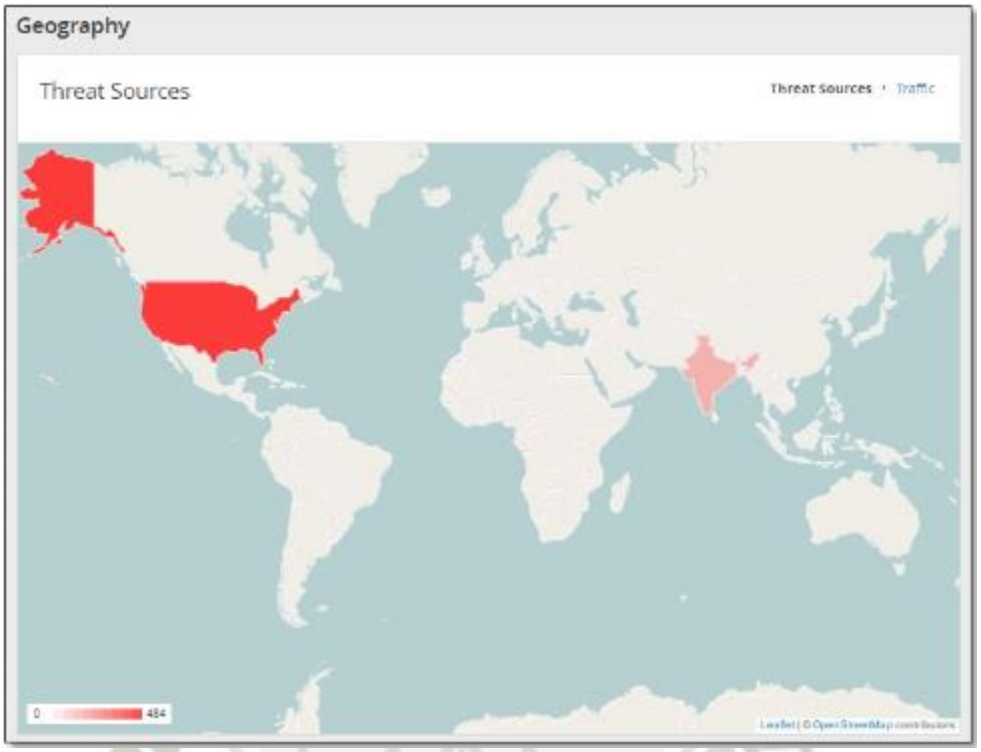
La verificación de integridad del navegador CloudFlare busca los encabezados HTTP comunes que son más utilizados por los spammers y automáticamente niega el acceso a su página. También desafiará a los visitantes que no tengan un agente de usuario o agente de usuario no estándar, también comúnmente utilizado por cunas, rastreadores o visitantes.

3. Desafío humano:

Los visitantes fueron presentados con una página de desafío CAPTCHA y no pudo pasar.

Una página CAPTCHA es una palabra difícil de leer o conjunto de números que sólo un humano puede traducir. Si se ingresó incorrectamente, la solicitud se bloquea.

Figura 19: Origen de los Ataques



Fuente: Resultados Cloudflare

Figura 20: Cantidad de Ataques por Zonas

Top Threat Origins

Last 24 Hours

Country	Requests
United States	484
India	162
Russian Federation	2
Norway	1

Fuente: Resultados Cloudflare

2.5.2. Pruebas de estrés

El ambiente de la prueba consiste en un entorno distribuido virtualizado, donde se encuentra un servicio SaaS (Visual Studio Team Services) que simula la conectividad de usuarios virtuales y los navegadores más concurrentes (Internet Explorer, Google Chrome y Firefox).

Prueba de estrés del Portal Web, la cual implica ingresar a www.senace.gob.pe.

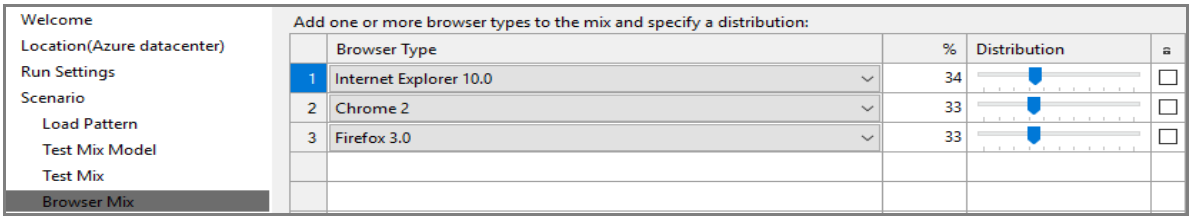
- **Detalle de Hardware a utilizar**

Componente	Hardware
1VM Windows SDD (PortalWeb)	4cores – 7 GB RAM

- **Simulación de Navegadores**
  - Internet Explorer 10.0
  - Chrome 2.0
  - Firefox 3.0

Con la finalidad de crear un ambiente que se asemeje a una situación real, se diseñó una distribución equivalente por cada navegador.

Figura 21: Distribución de Navegadores

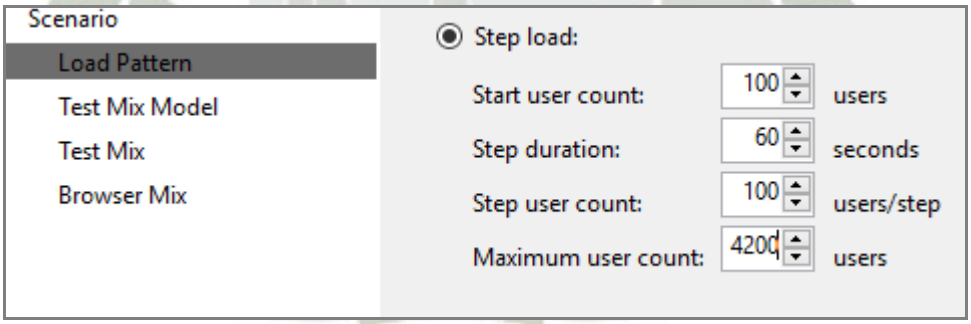


Fuente: Elaboración Propia

- **Carga de Usuarios**

Se ejecutó con un patrón de carga escalonada, iniciando con 100 usuarios, incrementados en 100 usuarios cada 60 segundos tal cual muestra la siguiente imagen.

Figura 22: Carga de Usuarios



Fuente: Elaboración Propia

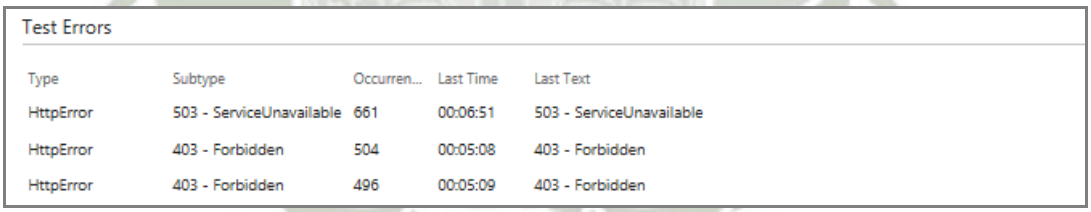
Esta configuración nos ayuda a detectar la cantidad de usuarios concurrentes que soporta el servicio "Portal Web" bajo un escenario completo.

Durante el análisis de errores, se verificó lo siguiente:

Hora	Error	Usuarios	Descripción
05:08	504	200	La página del portal llama a dicho archivo: **https://video.flim5-2.fna.fbcdn.net/v/t43.1792-2/19841930_1440852019296332_8718175044078927872_n.mp4-----{GET}**
05:09	504	200	La página del portal llama a dicho archivo: **https://video.flim5-2.fna.fbcdn.net/v/t43.1792-2/19841824_137810646800292_1212202395572895744_n.mp4-----{GET}**

- La siguiente imagen muestra los errores del servicio web.

- *Figura 23:*Errores del Servicio



Fuente: Elaboración Propia

Procedemos a realizar una prueba de estrés, con tipo de hardware diferente a la primera prueba.

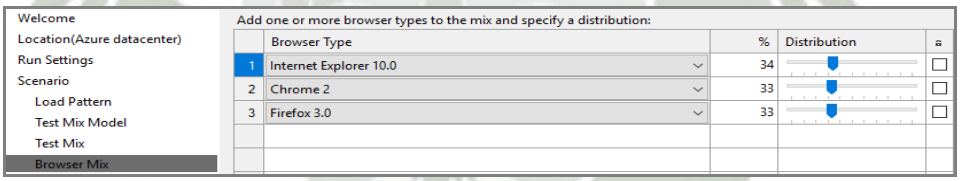
- **Las características de hardware utilizadas son:**

Componente	Hardware
1VM Windows SDD (PortalWeb)	8 cores – 16 GB RAM

- **Simulación de Navegadores**
  - Internet Explorer 10.0
  - Chrome 2.0
  - Firefox 3.0

Se recreó un ambiente de distribución equivalente por cada navegador.

Figura 24: Distribución de Navegadores

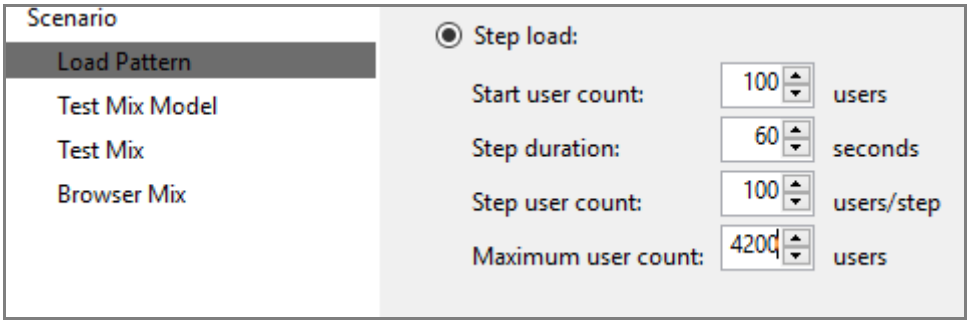


Fuente: Elaboración Propia

- **Carga de Usuarios**

Se ejecutó con un patrón de carga escalonada, iniciando con 100 usuarios, incrementándose en 100 usuarios cada 60 segundos tal cual muestra la siguiente imagen.

Figura 25: Carga de Usuarios



Fuente: Elaboración Propia

Esta configuración nos ayuda a detectar la cantidad de usuarios concurrentes que soporta el servicio de "Portal Web" alojado en Microsoft Azure**.**

Durante el análisis de errores, se verificó lo siguiente:

Hora	**Error**	**Usuarios**	**Descripción**
06:45	500	300	El portal web falla al llamar al siguiente archivo: **https://video.flim5-2.fna.fbcdn.net/v/t43.1792-2/19841824_137810646800292_1212202395572895744_n.mp4----{GET}**
06:44	500	300	El portal web falla al llamar al siguiente archivo: **https://video.flim5-2.fna.fbcdn.net/v/t43.1792-2/19841930_1440852019296332_8718175044078927872_n.mp4----{GET}**

- La siguiente imagen muestra los errores del servicio web.

- *Figura 26:* Errores de Servicio

Test Errors

Type	Subtype	Occurren...	Last Time	Last Text
Exception	WebTestException	862	00:14:16	Context parameter 'FormPostParam1.u_his' not found in test context
HttpError	403 - Forbidden	500	00:06:45	403 - Forbidden
HttpError	403 - Forbidden	500	00:06:44	403 - Forbidden

Fuente: Elaboración Propia

En las pruebas de rendimiento se evidenciaron 5 URLs cuyo tiempo de respuesta son bajos.

Figura 27: URLs con tiempo bajos de repuesta

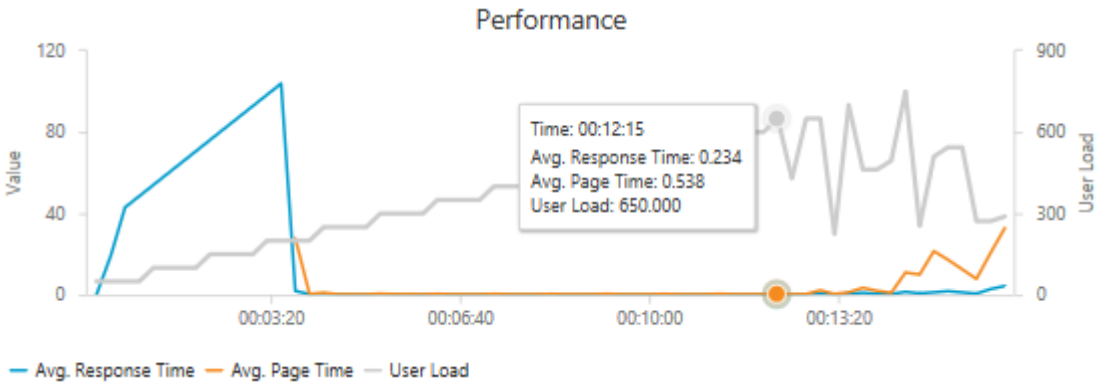
Top 5 slowest pages

Page URL	Scenario	Test	Avg. Page Time(sec) ↓	95th Percentile	Total Pages	% Pages Meeti...
http://www.pronis.gob.pe/----{GET}	Scenario1	WebTest1	10.929	57.823	5135	100
https://www.facebook.com/v2.3/plugins/page.php----{GET}	Scenario1	WebTest1	1.289	4.155	4183	100
https://video.flim5-2.fna.fbcdn.net/v/t43.1792-2/19841930_144085...	Scenario1	WebTest1	0.736	2.453	3840	100
https://www.facebook.com/ajax/bz----{POST}	Scenario1	WebTest1	0.482	0.956	3350	100
https://staticox.facebook.com/connect/xd_arbiter/r/XBwzv5Yrm_1.j...	Scenario1	WebTest1	0.481	1.329	4140	100

Fuente: Elaboración Propia

Performance ideal: El tiempo de respuesta ideal para 650 usuarios concurrentes es 0.234 segundos.

Figura 28: Gráfico de Concurrencia



Fuente: Elaboración Propia

Indicador	Solución(1Web)
Promedio de solicitudes por minuto	51 000
Carga de usuarios	650

Los puntos de mejora que elevarán la ratio de usuarios concurrentes en el servicio Encuestas serían:

- Realizar un tunning del servidor web, la cual le permita aprovechar la totalidad de su hardware y mejorar el performance.

En base a las pruebas de estrés, se concluye que:

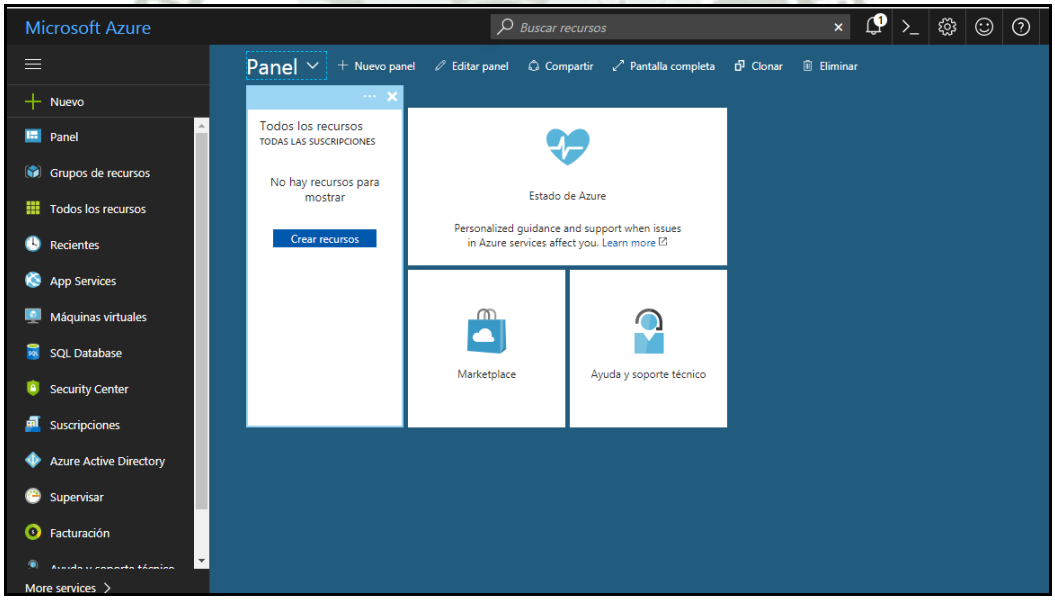
- El flujo completo del portal web, soporta 2000 usuarios concurrentes, generando 26 056 solicitudes por minuto
- En la prueba N°2 debido a la fluctuación de usuarios, se recomienda revisar el archivo de configuración con la finalidad de optimizar los tiempos de respuesta y comportamiento de la misma.

2.6. Manuales de Usuarios

Para poder administrar la infraestructura creada alojada en la plataforma de Azure, lo primero que debe considerarse es el nombre de la suscripción y su estado, para ello, el usuario deberá de abrir un navegador y digitar la siguiente dirección: http://portal.azure.com y acceder con sus respectivas credenciales.

En el portal de Azure (Figura 29), el usuario podrá observar que cuenta con una estructura respecto a los servicios migrados a la nube, es por eso que lo primero que debe hacerse, es ubicar el grupo al que pertenece el servidor al que nos vamos a conectar.

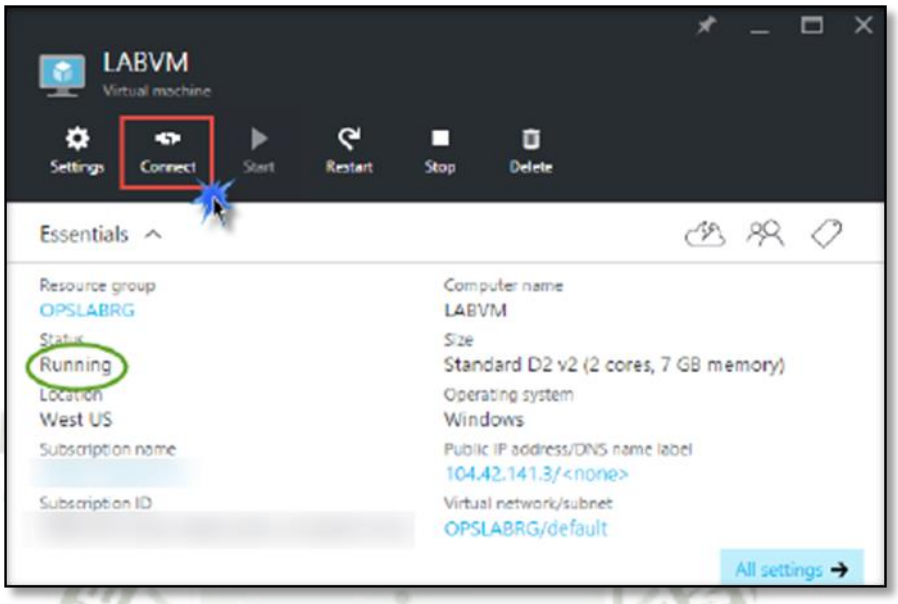
Figura 29: Pantalla principal de ingreso a Microsoft Azure



Fuente: Elaboración Propia

Una vez encontrado, el usuario procederá a abrir los detalles en configuración y a hacer clic en conectar al servidor (Figura 30).

Figura30: Propiedades de servidor alojado en Azure

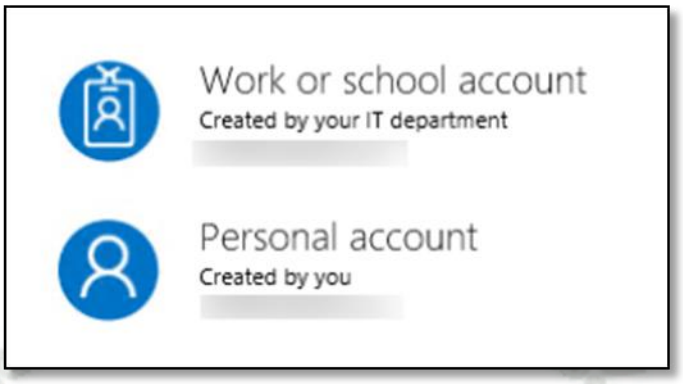


Fuente: Elaboración Propia

Después de conectarse a través del escritorio remoto, el usuario debe abrir el navegador de internet Explorer, ya que este viene por defecto en el sistema del servidor, caso contrario podrá descargar el navegador de su preferencia.

Allí digita e ingresa a la siguiente URL: https://portal.azure.com y procede a autenticarse con su cuenta organizacional o por cuenta de Microsoft (Figura 31).

Figura 31: Tipos de cuentas para la autenticación.



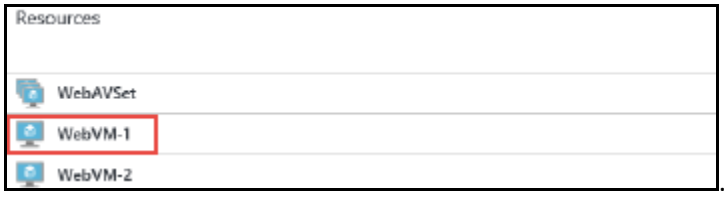
Fuente: Elaboración Propia

Una vez que ingrese a su cuenta, en paralelo dentro del servidor, se mostrará como poder hacer uso de las extensiones de la máquina virtual (Figura 32) y personalizarlas de acuerdo a sus necesidades.

Lo primero que se debe hacer es abrir el grupo de recursos, en este caso con el nombre de OpsVMRmRG, haciendo clic en grupos de recursos y luego haciendo clic en el nombre del grupo de recursos. También se puede acceder haciendo clic en Examinar -> Grupos de recursos.

Una vez que se encuentra dentro del grupo de recursos, se procede a hacer clic en la máquina virtual llamada WebVM-1.

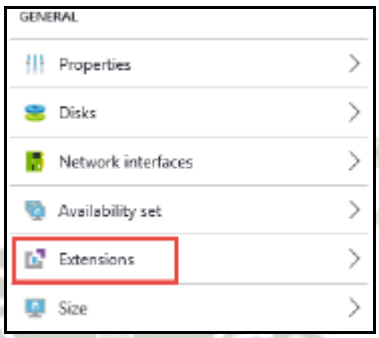
Figura 32: Relación de máquinas virtuales en el grupo de recursos.



Fuente: Elaboración Propia

En la parte izquierda, se muestra una hoja de configuración perteneciente a la máquina virtual, es allí donde el usuario procede a hacer clic en la opción de extensiones (Figura 33).

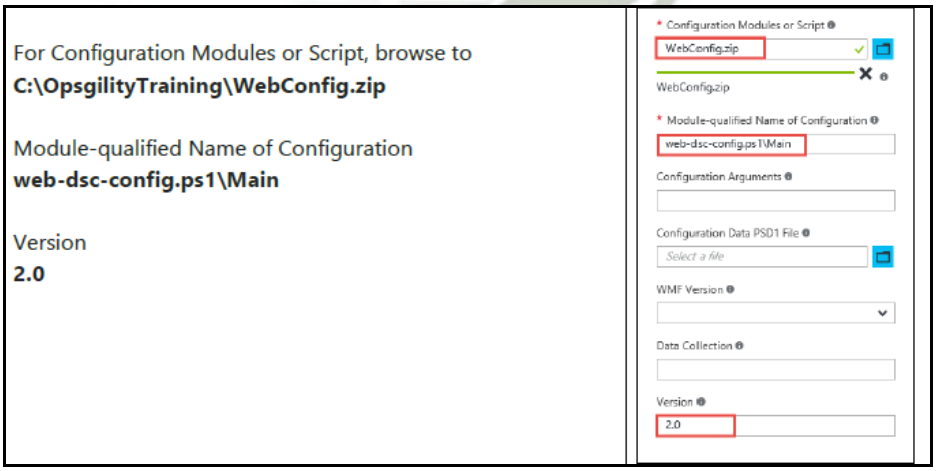
Figura 33: Configuración de extensiones para la VM



Fuente: Elaboración Propia

Dentro de la opción extensiones se debe especificar las siguientes configuraciones, en este caso destinadas para la máquina virtual que contiene el entorno web del aplicativo (Figura 34), una vez especificadas el usuario da clic en OK.

Figura 34: Especificaciones de las extensiones para Web

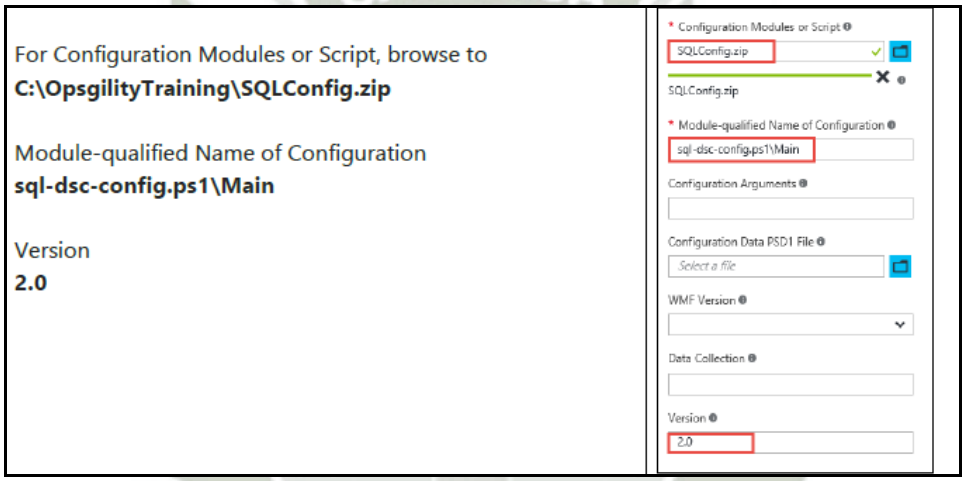


Fuente: Elaboración Propia

Después de las actualizaciones de cambio, el usuario podrá hacer lo mismo para la máquina virtual que contiene la base de datos del aplicativo y procederá a repetir todos los pasos anteriores desde la selección de la máquina en el grupo de recursos (Figura 35), que en este caso se llama SQLVM-1.

Una vez que el usuario ubica la máquina virtual y realiza las respectivas configuraciones, se continúa con la opción de extensiones, donde de igual manera especificar las siguientes configuraciones.

Figura 35: Especificaciones de las extensiones para SQL



Fuente: Elaboración Propia

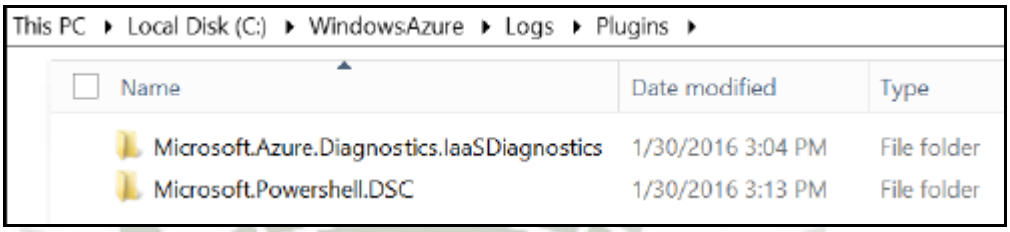
Desde el interior de la máquina virtual, el usuario podrá hacer clic en el icono Explorador de archivos:

Figura 36: Icono del Explorador de archivos en Windows Server

Fuente: Elaboración Propia

Para poder ingresar a la carpeta llamada Plugins en: C: \ Windows Azure \ Logs. Aquí es donde se almacena la máquina virtual y los archivo de registros de extensión anteriormente configurados, y también es el punto de partida para las extensiones de solución de problemas (Figura 37).

Figura 37: Carpetas contendoras de registros de extensión



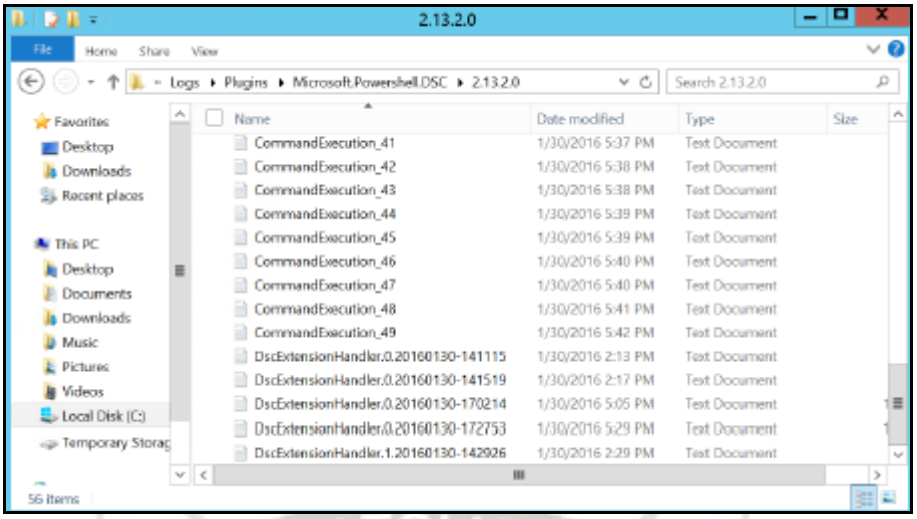
Fuente: Elaboración Propia

El usuario seleccionará la carpeta Microsoft.PowerShell.DSC \ 2.X para poder revisar algunos de los archivos de registro utilizando el bloc de notas. Esta carpeta contiene los archivos de registro para la extensión PowerShell DSC que sirven para la personalización de la máquina virtual (Figura 38).

El CommandExecution * son los archivos de registro del código de controlador, que ejecuta el script DSC.

Los * DscExtensionHandler son los archivos de registro de la propia escritura de DSC.

Figura 38: Archivos de registros del servidor WebVM-1



Fuente: Elaboración Propia

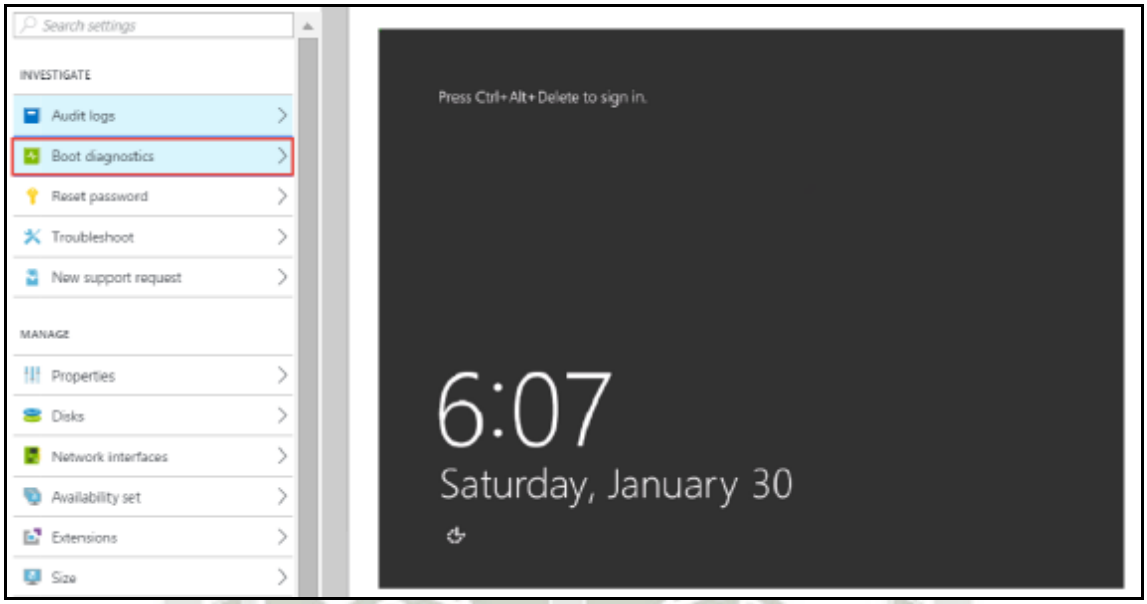
Si se produce un error durante la ejecución, gracias al detalle de la extensión, el usuario podrá verificar los detalles en los archivos de registro.

Después de los guiones que se han ejecutado y validando que el sitio cargue mediante la apertura de la hoja de configuración para WebVM-1 en el Portal de administración de Azure (Figura 39).

El usuario podrá habilitar la opción de diagnóstico y monitoreo, primero revisará el diagnóstico de arranque, que se encuentra dentro del portal de Azure, abriendo la máquina virtual WebVM-1.

En la configuración de las opciones haga clic en diagnóstico de arranque para ver una captura de pantalla de la consola. Esto puede ser útil para solucionar problemas de inicio de su máquina virtual.

Figura 39: Diagnóstico de arranque



Fuente: Elaboración Propia

Ahora, para poder realizar una configuración de alerta (Figura 40), nos situamos dentro de la hoja de configuración WebVM-1 y se da clic en alerta de reglas.

Figura 40: Alertas de reglas

Fuente: Elaboración Propia

El usuario deberá especificar la siguiente configuración de la regla de alerta:

a. Nombre: Alerta de la CPU

b. Descripción: Alerta de Alto uso de la CPU

c. Métricas: Porcentaje de la CPU del sistema operativo invitado

d. Condición: Mayor que

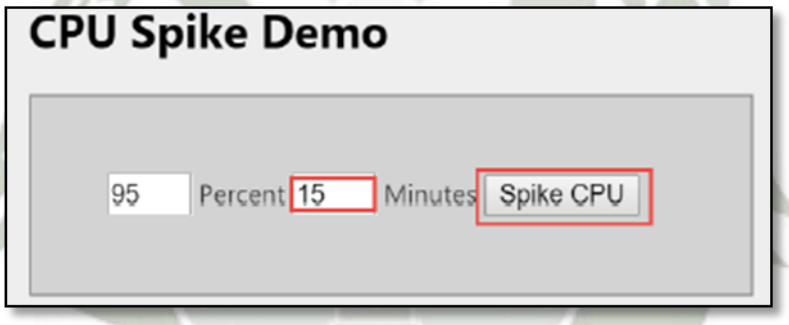
e. Umbral: 25

f. Período: Durante los últimos 5 minutos

g. Los correos electrónicos adicionales de administrador: especifique su dirección de correo electrónico aquí para recibir la notificación.

Se desplazará hacia abajo en la página de la sección de la CPU del punto de demostración (Figura 41). Se coloca en minutos a 15 y se hace clic en punto de la CPU.

Figura 41: Configuración de la regla de alertas de CPU



Fuente: Elaboración Propia

Después de 5-15 minutos recibirá un correo electrónico de alerta notificar la alerta se activó (Figura 42). Después de un tiempo el usuario recibirá una segunda notificación señalando que el problema se ha resuelto (después de aplicar gotas de uso de CPU).

Alert notification email	Alert resolution email

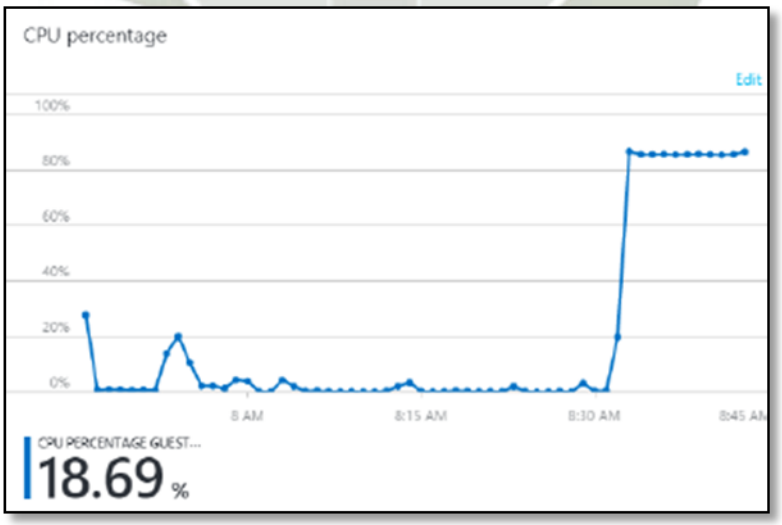
Figura 42: Confirmación de la configuración de alertas

▲ 'CPU percentage guest OS GreaterThan 25 (Percent) in the last 5 minutes' was activated for virtualMachines: WebVM-1 (OpsVMRmRG)	✓ 'CPU percentage guest OS GreaterThan 25 (Percent) in the last 5 minutes' has been resolved for virtualMachines: WebVM-1 (OpsVMRmRG)

Fuente: Elaboración Propia

El azulejo de supervisión (Figura 43) también deberá mostrar la utilización de aumento de la CPU:

Figura 43: Gráfico del uso de CPU



Fuente: Elaboración Propia

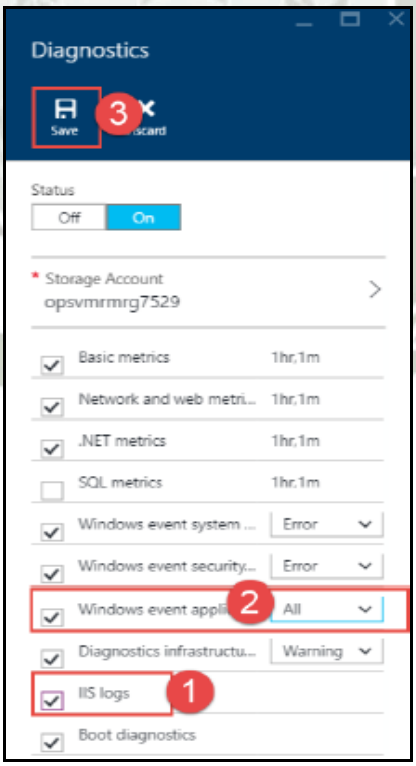
Ahora, para poder configurar un registro de captura de registros de IIS, no situamos dentro de la hoja de configuración WebVM-1 y se dará clic en diagnósticos.

Figura 44: Opción de diagnósticos

Fuente: Elaboración Propia

En la hoja de diagnóstico, marque la casilla de registros de IIS, y cambiar los registros de aplicación por sucesos de Windows (Figura 45), esto para todos, y luego hacer clic en el botón guardar de la barra de herramienta.

Figura 45: Hoja de especificaciones de diagnósticos

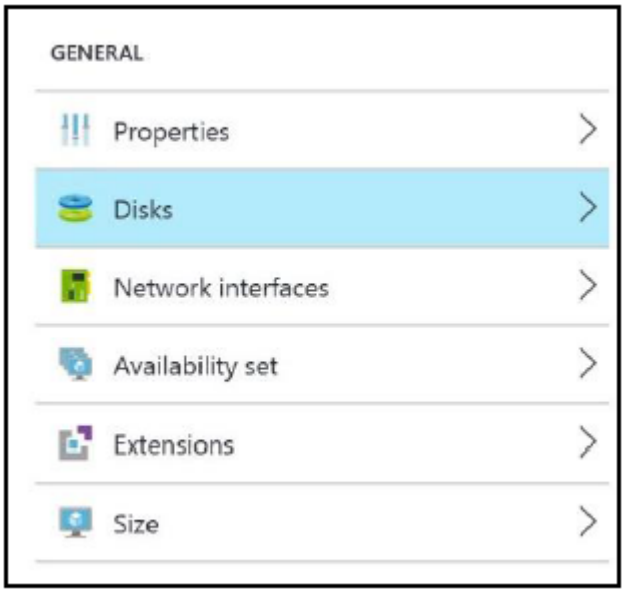


Fuente: Elaboración Propia

Para contar con almacenamiento de conexión adicional (Figura 46), el usuario deberá situarse en el portal de gestión de Azure, y hacer clic en examinar, máquinas virtuales y hacer clic en WebVM-1

En la hoja configuración, en la sección general, hacer clic en discos.

Figura 46: Opción de discos.



Fuente: Elaboración Propia

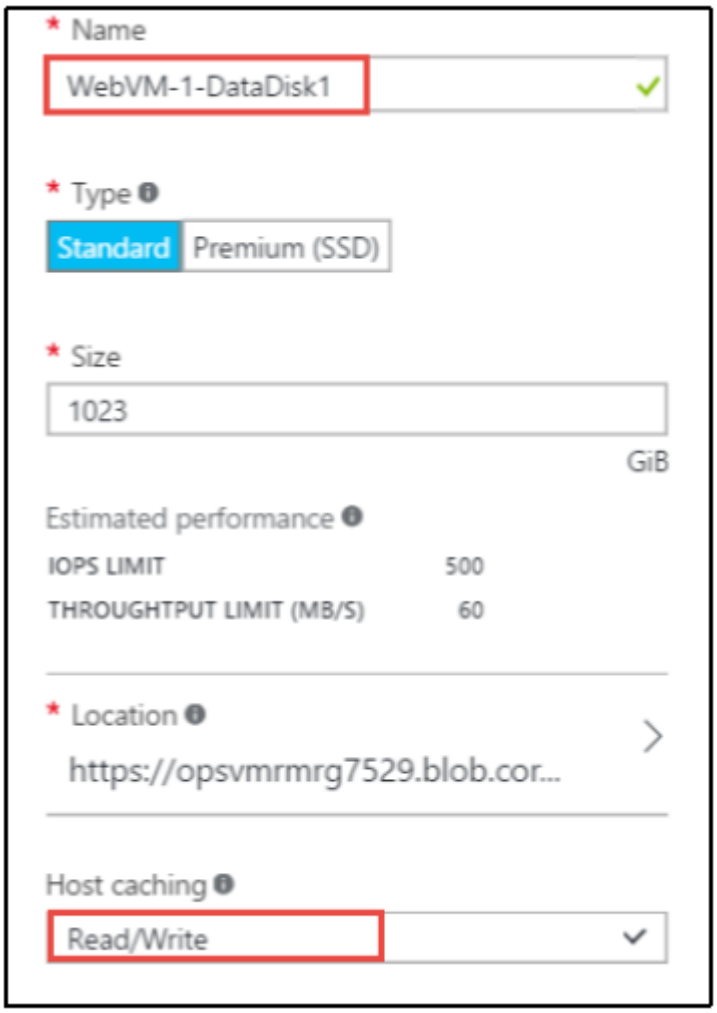
El usuario deberá hacer clic en nuevo almacenamiento (Figura 47).

Figura 47: Opción para adjuntar disco nuevo o existente.

Fuente: Elaboración Propia

Así podrá definir el nombre del disco, que en este caso se llamará WebVM-1-DataDisk 1, y cambiar el almacenamiento en caché al anfitrión para lectura y escritura (Figura 48). Luego dar clic en OK para conectar el disco.

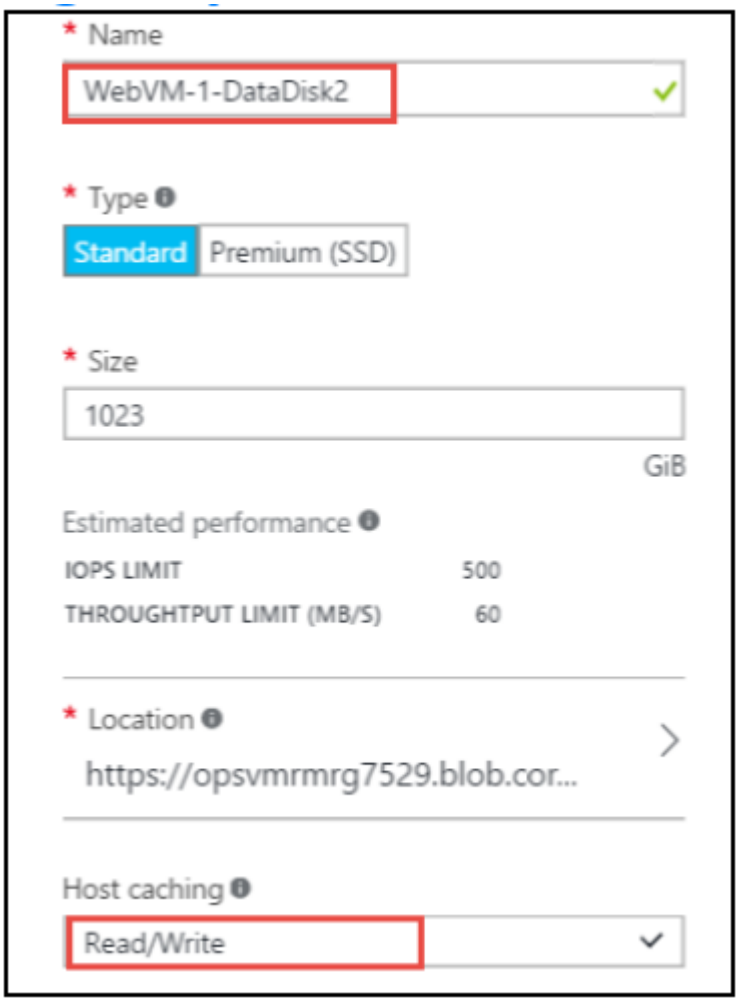
Figura 48: Especificaciones del primer disco adjuntar.



Fuente: Elaboración Propia

Para un segundo disco de almacenamiento, se repite el proceso y el nombre del segundo disco en este caso será WebVM-1-DataDisk 2 (Figura 49).

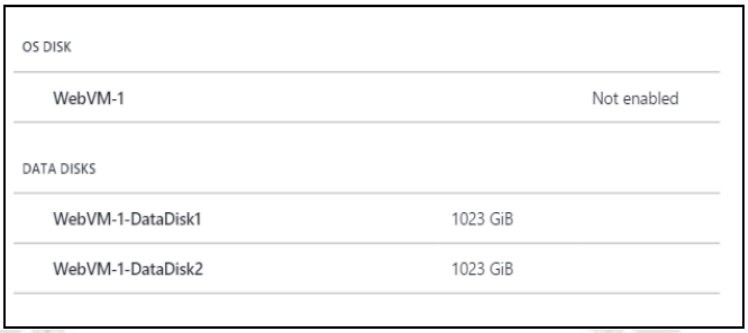
Figura 49: Especificaciones del segundo disco a adjuntar.



Fuente: Elaboración Propia

La configuración de disco debe ser similar a la siguiente:

Figura 50: Listado de discos



Fuente: Elaboración Propia

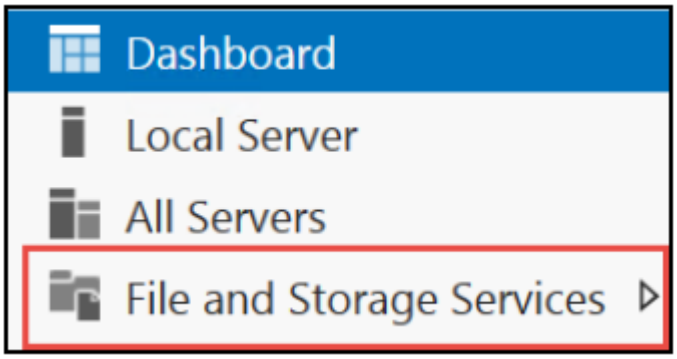
Después de las anteriores configuraciones, procedemos a crear un nuevo espacio de almacenamiento para los discos dentro del entorno virtual, el usuario deberá hacer clic en el botón del administrador del servidor Windows (Figura 51).

Figura 51: Administrador del servidor Windows

Fuente: Elaboración Propia

Buscar la opción de servicios de archivos y almacenamiento dentro de administrador de Windows Server (Figura 52).

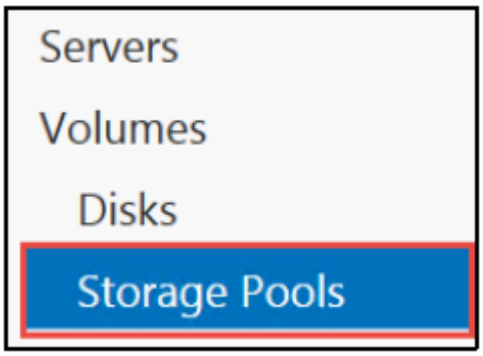
Figura 52: Servicios de archivos y almacenamiento



Fuente: Elaboración Propia

Y una vez dentro de la opción seleccionada, el usuario deberá buscar y hacer clic en agrupaciones de almacenamiento (Figura 53).

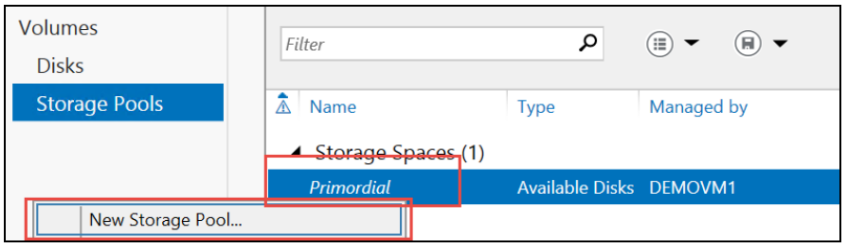
Figura 53: Opción de agrupaciones de almacenamiento



Fuente: Elaboración Propia

El usuario deberá hacer clic derecho en la columna de discos primordial, y luego hacer clic en nuevo grupo de almacenamiento (Figura 54).

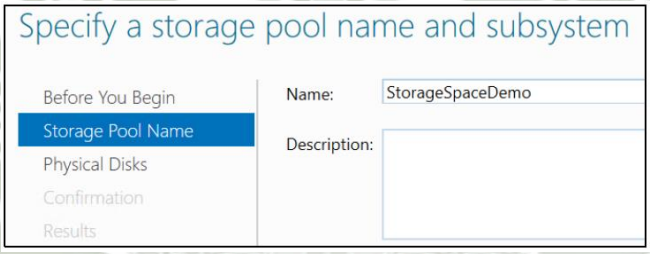
Figura 54: Panel para configuraciones de discos



Fuente: Elaboración Propia

Se procede a especificar el nombre, en este caso se llamará StorageSpaceDemo y hacer clic en siguiente (Figura 55).

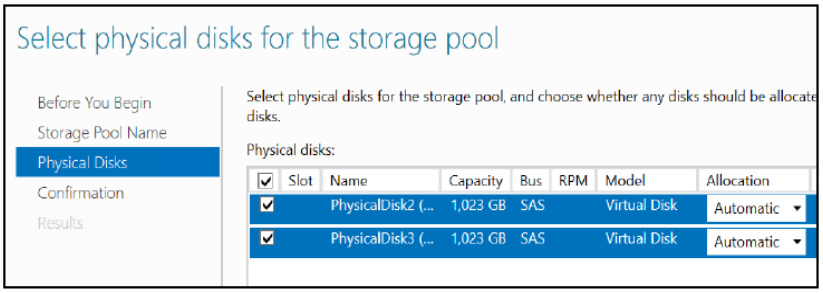
Figura 55: Especificaciones de almacenamiento



Fuente: Elaboración Propia

Después se selecciona los dos discos que se adjuntaron y se hace clic en siguiente (Figura 56).

Figura 56: Detalle de los discos existentes.

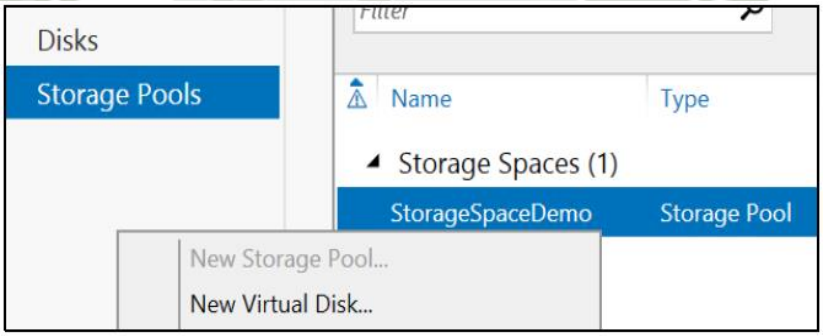


Fuente: Elaboración Propia

En la fase de confirmación, hacer clic en crear y luego en cerrar, después se creará el espacio de almacenamiento (Figura 57).

Se continúa haciendo clic derecho en el nuevo espacio de almacenamiento y luego hacer en la opción de nuevo disco virtual.

Figura 57: Distribución del espacio de almacenamiento.

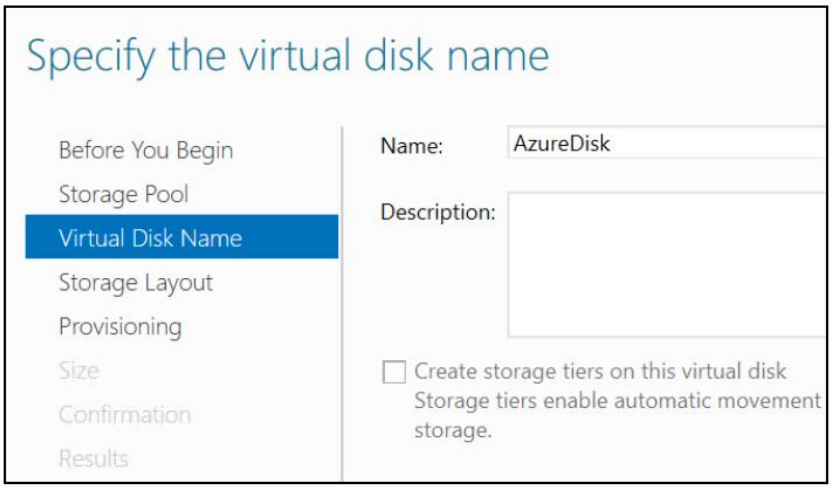


Fuente: Elaboración Propia

El usuario deberá hacer clic en siguiente, y en el cuadro de diálogo, todo esto antes de comenzar, y seleccionar el grupo de almacenamiento creado anteriormente.

Nombre del disco y haga clic en Siguiente (Figura 58).

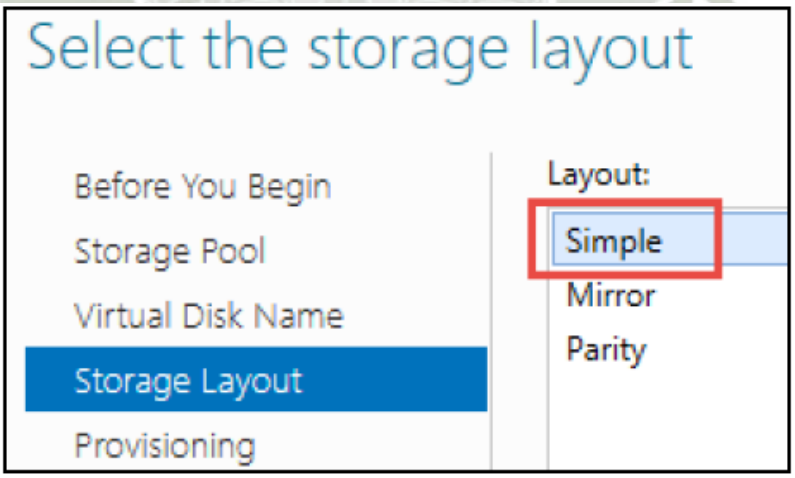
Figura 58: Pantalla para especificación del nuevo disco



Fuente: Elaboración Propia

A continuación se debe seleccionar la distribución de almacenamiento simple y a clic en siguiente para continuar (Figura 59).

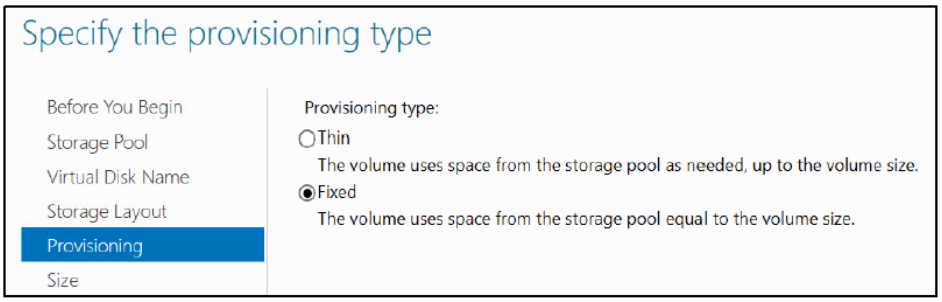
Figura 59: Pantalla para el tipo de partición del disco.



Fuente: Elaboración Propia

Aceptar el valor predeterminado fijo (Figura 60).

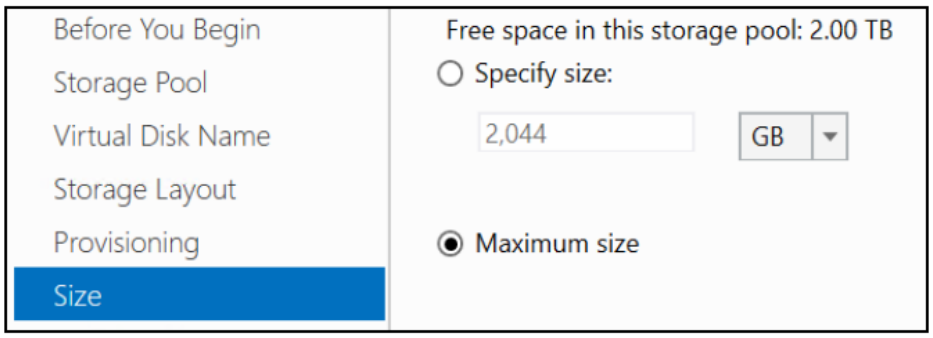
Figura 60: Opción de especificación del tipo de aprovisionamiento.



Fuente: Elaboración Propia

Cambiar el tamaño de tamaño máximo (Figura 61).

Figura 61: Distribución de tamaño de disco

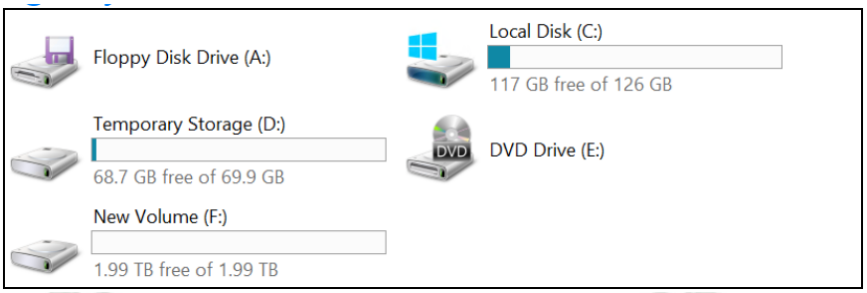


Fuente: Elaboración Propia

El usuario deberá hacer clic en la opción crear del cuadro de diálogo para confirmar y completar el asistente del nuevo volumen de disco y aceptar la configuración predeterminada para todos los diálogos.

Al final, se podrá observar (Figura 62) que se tiene un nuevo volumen de 2 TB repartidas en dos discos.

Figura 62: Unidades de almacenamiento.

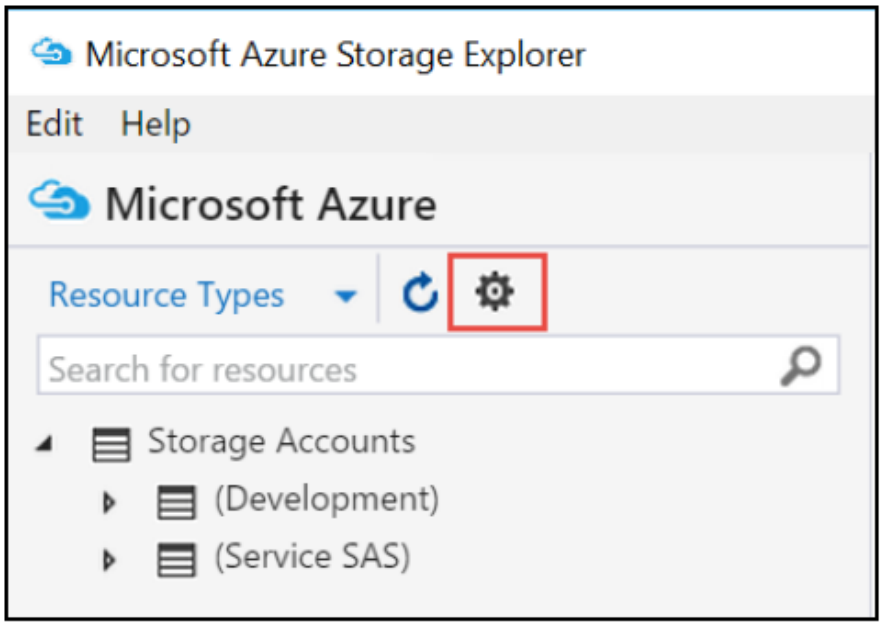


Fuente: Elaboración Propia

Para poder continuar, el usuario se deberá desconectar de la sesión de escritorio remoto.

En el escenario donde se tiene 2 o más máquinas virtuales que comparten una cuenta de almacenamiento y el usuario requiera de una sincronización de archivos. Debe utilizar la herramienta Microsoft Azure Storage Explorer, y se procederá a hacer clic en el engranaje para configurar el acceso a la suscripción Azure (Figura 63).

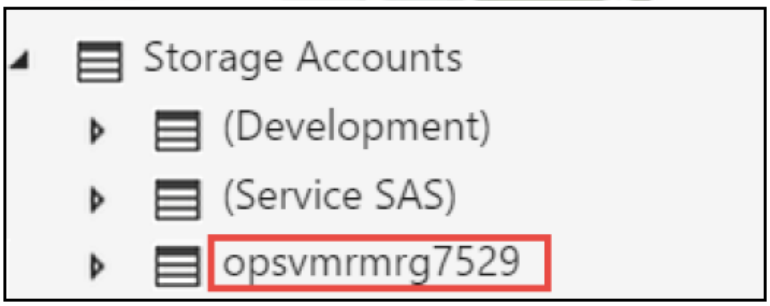
Figura 63: Pantalla de inicio de la herramienta Microsoft Azure Explorer



Fuente: Elaboración Propia

El usuario deberá añadir su cuenta de la sesión con las credenciales de su suscripción Azure y hacer clic en la cuenta de almacenamiento (Figura 64) utilizado por las máquinas virtuales ya mencionadas anteriormente.

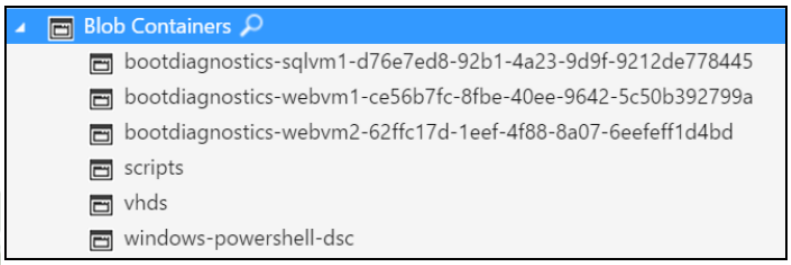
Figura 64: Lista de cuentas de almacenamiento.



Fuente: Elaboración Propia

Se expande el blob de los contenedores que muestra el diagnóstico de arranque. Allí se podrá observar el contenedor de secuencias de comandos, donde se ha subido la extensión script personalizada para el contenedor (Figura 65), ventanas de PowerShell-DSC DSC y finalmente el contenedor VHD, donde se almacenan los archivos de disco duro virtual para sus máquinas virtuales.

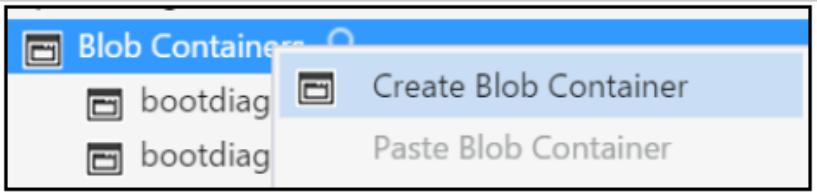
Figura 65: Archivos pertenecientes al contenedor de blob.



Fuente: Elaboración Propia

El usuario deberá hacer clic derecho en el nodo envases blob y luego en crear contenedor de blob (Figura 66).

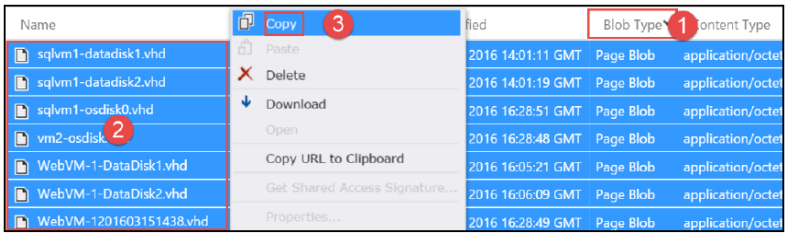
Figura 66: Creación de contenedor de blob.



Fuente: Elaboración Propia

Luego se debe hacer doble clic en el contenedor VHD para ver su contenido y luego ordenar por tipo blob hasta que la página quede en primer lugar y así seleccionar todos los elementos de página blob (Figura 67), hacer clic derecho y copiar.

Figura 67: Método de copia de todos los elementos de la página blob.



Fuente: Elaboración Propia

Haga doble clic en el contenedor de copias de disco, después de que este se abra, hacer clic en pegar en la barra de herramientas (Figura 68).

Figura 68: Barra de herramientas del contenedor de discos.

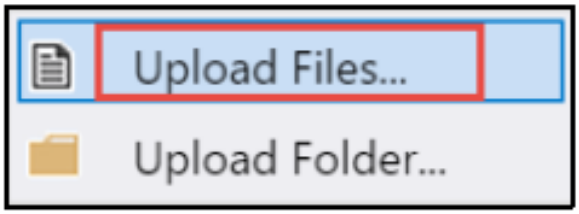
Fuente: Elaboración Propia

Dentro de la utilidad del aplicativo de almacenamiento Azure, se puede abrir el contenedor VHD de la cuenta de almacenamiento directo para su máquina virtual.

Se deberá hacer clic en el botón de cargar desde la barra de herramientas.

El usuario deberá hacer clic en el elemento de menú cargar archivos (Figura 69) y proceder con la actividad.

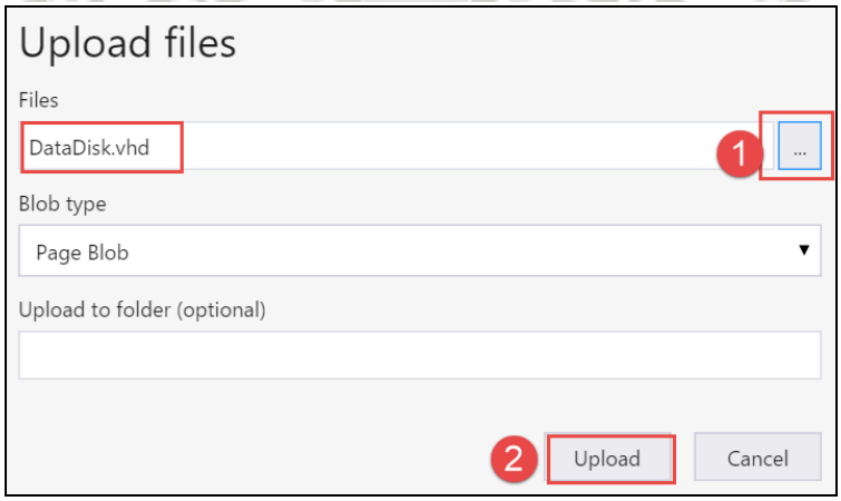
Figura 69: Subida de archivos



Fuente: Elaboración Propia

En el cuadro de diálogo cargar archivos, para esto deberá ir a C: \ Capacitación Opsgility \ Data Disk.vhd y hacer clic en cargar (Figura 70).

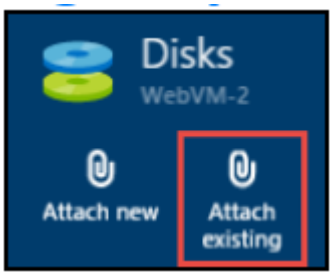
Figura 70: Detalle de archivos del tipo page blob



Fuente: Elaboración Propia

En el portal de administración de Azure, abrir la configuración de la máquina virtual de WebVM-2 haciendo clic en examinar, abrir discos y luego hacer clic en adjuntar existente (Figura 71).

Figura 71: Adjuntar disco existente.



Fuente: Elaboración Propia

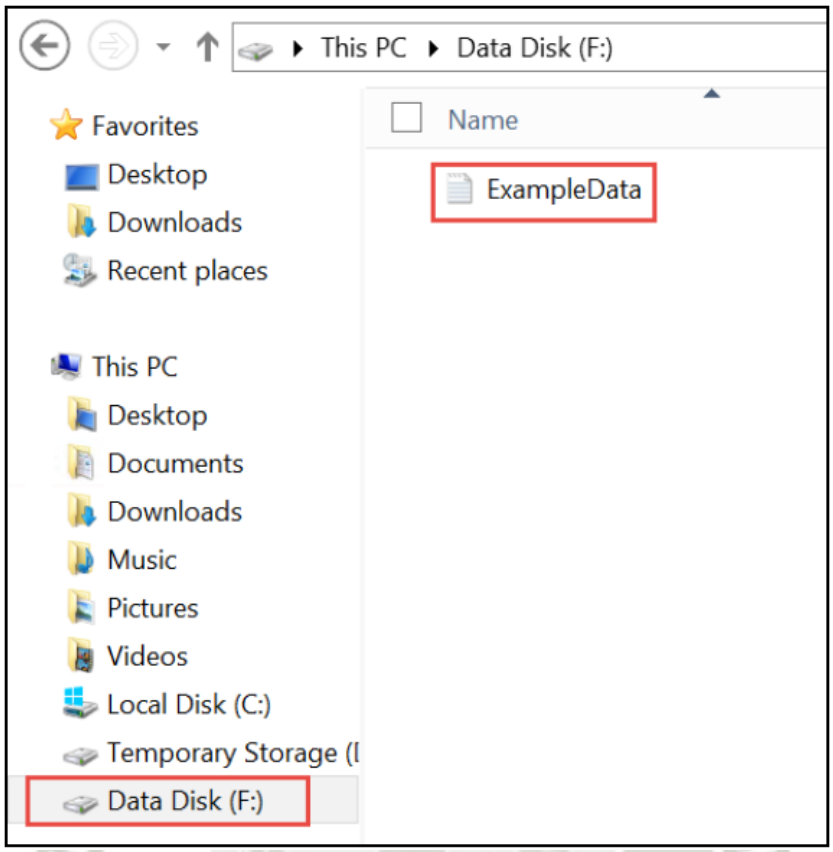
El usuario deberá continuar ingresando a la cuenta de almacenamiento que ha cargado el archivo de DataDisk.vhd, luego abrir el contenedor VHD, y seleccionar el archivo DataDisk.vhd (Figura 72), ubicarse en la parte inferior de la hoja y hacer clic en el botón seleccionar para adjuntar el disco de datos.

Figura 72: Características de archivo .vhd

Fuente: Elaboración Propia

Desde el interior de la máquina virtual WebVM-2 corroborar las configuraciones haciendo clic en el icono de explorador de archivos y navegar hasta la unidad F: (puede ser E :) teniendo en cuenta que el disco está unido con los datos cargados desde el disco duro virtual cargado (Figura 73).

Figura 73: Archivo cargado desde el VHD



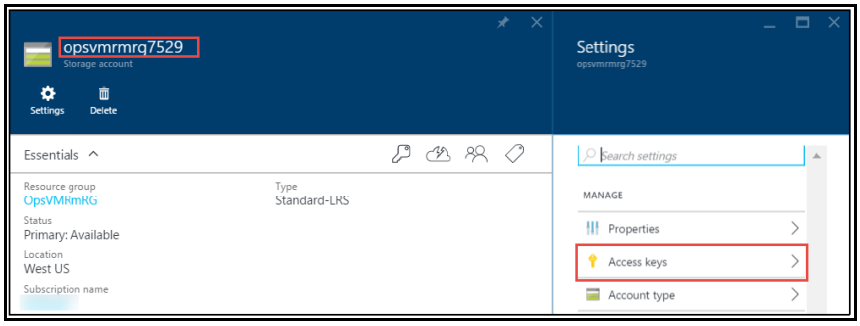
Fuente: Elaboración Propia

Para el diagnóstico de análisis de datos almacenados en Azure Storage, el usuario utilizará la aplicación llamada Azure Management Studio (AMS). Podrá descargarlo e instalar la versión de prueba del aplicativo de: http://www.cerebrata.com/.

La aplicación AMS requiere el nombre de cuenta y la clave de almacenamiento cuenta de almacenamiento. Copiar la clave con el lanzamiento del portal de administración de Azure, hacer clic en examinar, cuentas y depósitos, después hacer clic en la cuenta de almacenamiento creada anteriormente.

En la hoja de la cuenta de almacenamiento (Figura 74), digite el nombre de la cuenta de almacenamiento y haga clic en la tecla de acceso.

Figura 74: Herramientas de almacenamiento.



Fuente: Elaboración Propia

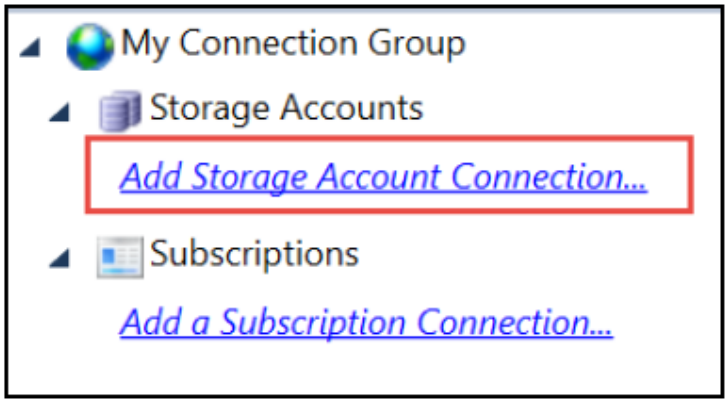
Una vez allí, el usuario deberá copiar el valor para KEY 1 (Figura 75).

Figura 75: Llaves de seguridad para el acceso

Fuente: Elaboración Propia

Dentro de la aplicación AMS, hacer clic en agregar conexión de la cuenta de almacenamiento (Figura 76).

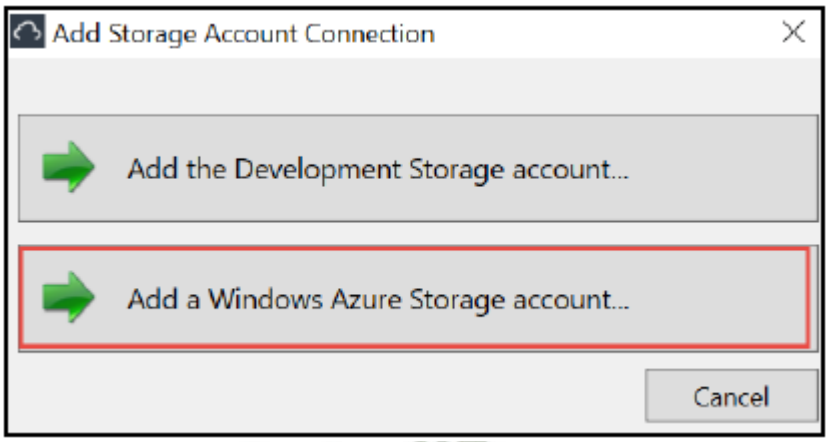
Figura 76: Panel del grupo de conexión.



Fuente: Elaboración Propia

Proceder y hacer clic en agregar una cuenta de almacenamiento de Windows Azure (Figura 77).

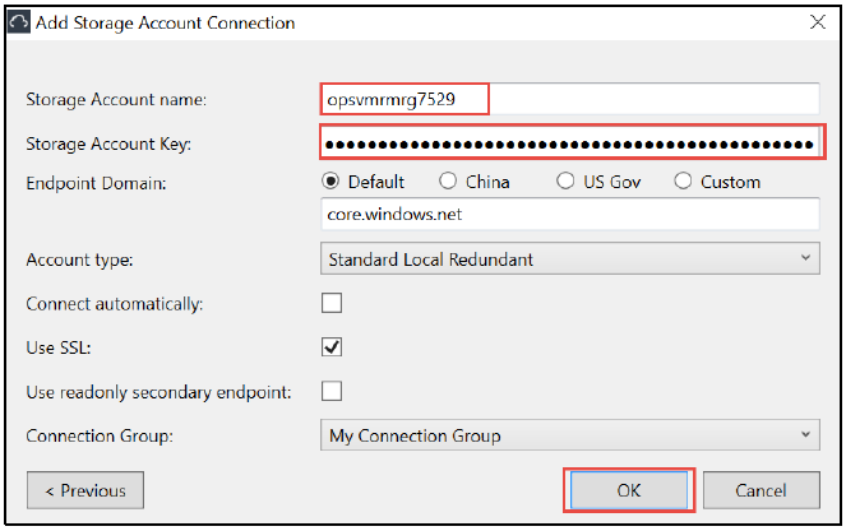
Figura 77: Opciones de las cuentas de almacenamiento.



Fuente: Elaboración Propia

El usuario deberá agregar el nombre de la cuenta de almacenamiento, y la clave de la misma en el cuadro de diálogo (Figura 78) y hacer clic en OK.

Figura 78: Agregar conexión para la cuenta de almacenamiento.

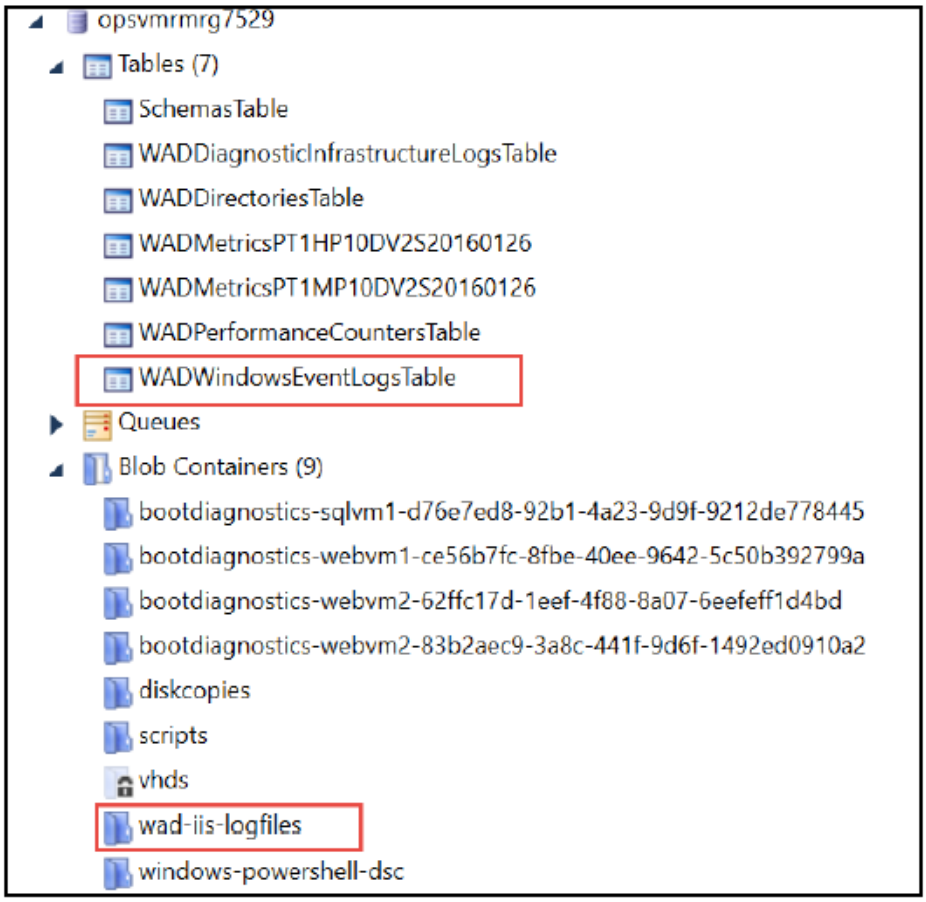


Fuente: Elaboración Propia

Expandir la cuenta de almacenamiento, y así expandir las tablas y los contenedores de blob (Figura 79). Esta es la ubicación de los datos almacenados para Azure Diagnósticos.

El WADWindowsEventLogsTable puede ser consultado para ver los registros de sucesos de la máquina virtual. Las tablas WADMetrics * contienen los contadores de rendimiento capturados en forma de datos. El contenedor taco-II-archivos de registro (contenedor blob bajo) almacena los archivos de registro de IIS, y si se configura a través de los archivos de registro adicionales de configuración XML podría ser capturado y almacenado en el almacenamiento de blob también.

Figura 79: Archivos del contenedor de almacenamiento.

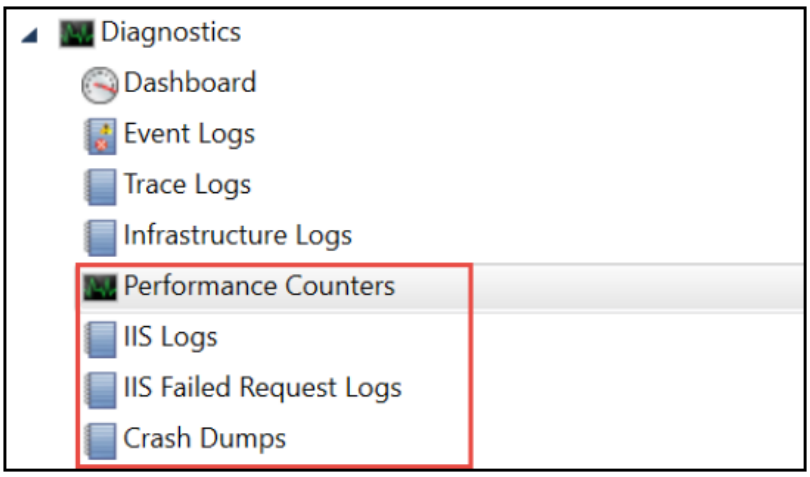


Fuente: Elaboración Propia

Después de la siguiente sincronización el usuario verá un nuevo contenedor (Figura 80) creado taco-II-archivos de registro con nombre.

El nodo de diagnósticos que aparece en ASM no es compatible con todos los datos de diagnóstico. Si se configura a través de XML puede capturar volcados por fallo, y en IIS los registros de errores de las solicitudes. En este ejemplo, se podrá ver los registros de IIS y contadores de rendimiento.

Figura 80: Contador de rendimiento perteneciente a diagnósticos.

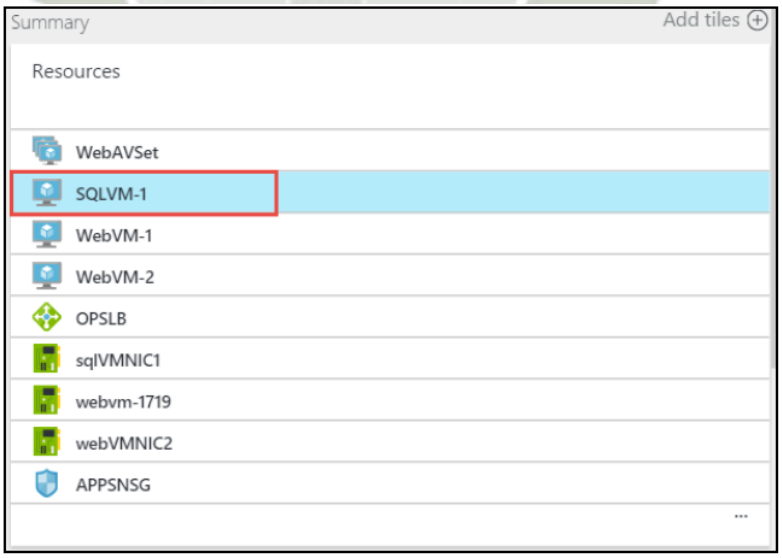


Fuente: Elaboración Propia

Se precederá a configurar la red de grupos de seguridad pública y el IPS.

Para poder añadir una dirección IP pública se debe hacer uso del portal de administración de Azure, hacer clic en examinar, grupos de recursos, (Figura 81) y en este caso hacer clic en la máquina virtual SQLVM-1.

Figura 81: Listado de componentes pertenecientes a un grupo de recursos.

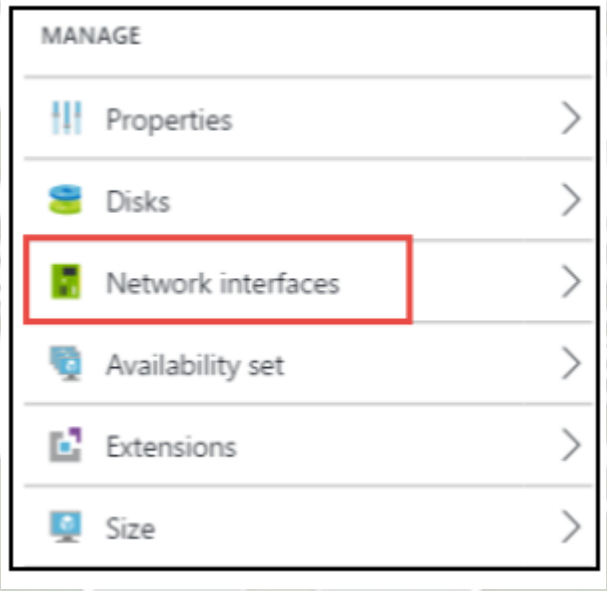


Fuente: Elaboración Propia

El usuario deberá tener en cuenta que el botón de conexión está desactivado en la barra de herramientas (Figura 82). Esto es porque no hay una dirección IP pública asociada con esta máquina virtual.

Para agregar una dirección IP pública, deberá hacer clic en el azulejo de interfaces de red del SQLVM-1 en la parte de configuración de la hoja.

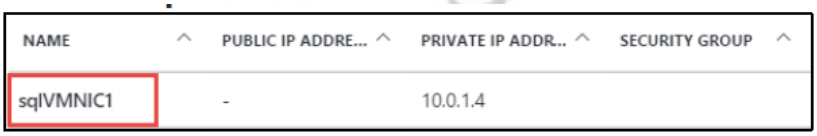
Figura 82: Interfaz de red.



Fuente: Elaboración Propia

Y hacer clic en la interfaz de red de SQL vmnic1 (Figura 83).

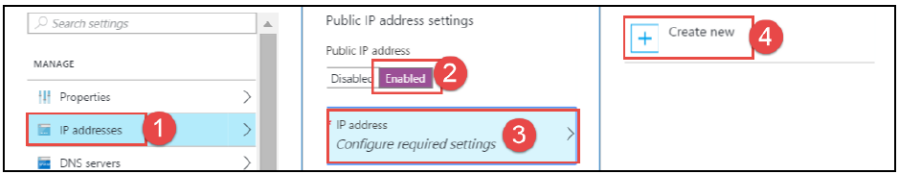
Figura 83: Características de la interfaz de red



Fuente: Elaboración Propia

A continuación, hacer clic en habilitado bajo dirección IP pública y en crear nuevo (Figura 84).

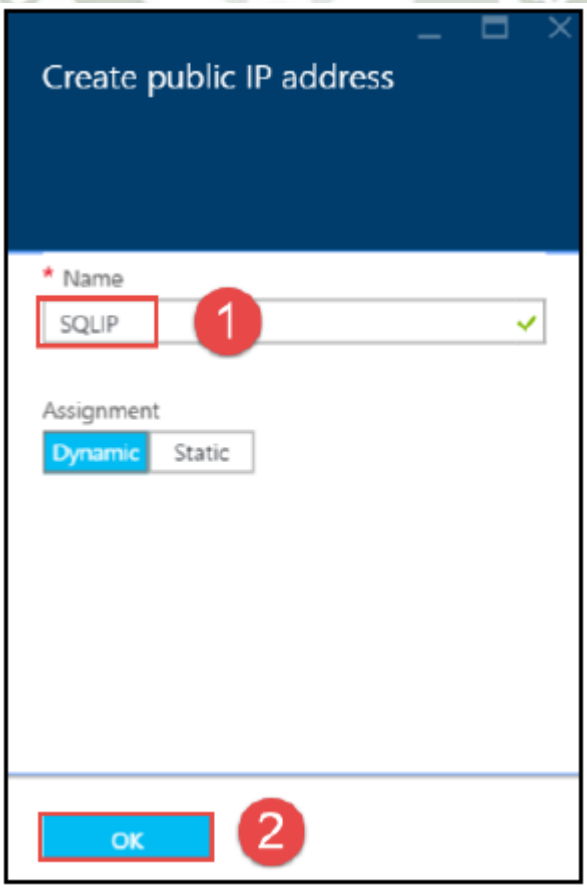
Figura 84: Configuraciones de IP



Fuente: Elaboración Propia

En la pantalla crear dirección IP pública, agregar el nombre, que en este caso será SQLIP IP (Figura 85) y hacer clic en OK.

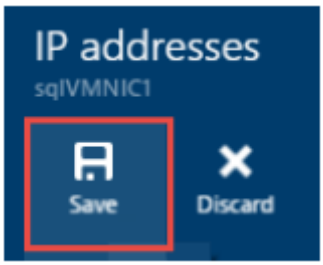
Figura 85: Creación de IP pública



Fuente: Elaboración Propia

Después se deberá hacer clic en guardar en la barra de herramientas (Figura 86) para así poder guardar la nueva dirección IP y asociarlo con la interfaz de red.

Figura 86: Guardar la IP pública



Fuente: Elaboración Propia

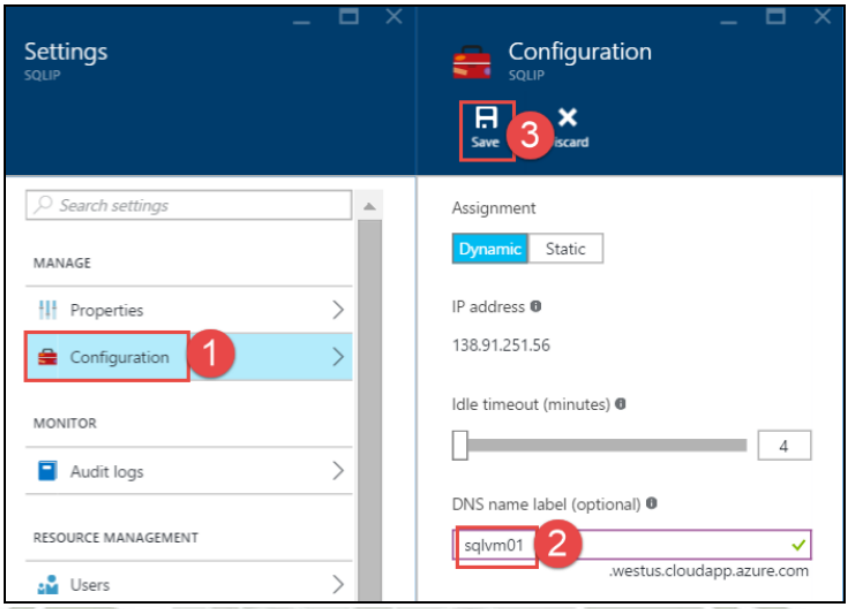
Una vez finalizado, aparecerá la notificación de actualización que muestra los cambios que han sido completados o fallidos (Figura 87), después de la confirmación el usuario podrá cerrar todas las ventanas de configuración de la máquina virtual.

Figura 87: Notificaciones del estado de cambios.

Fuente: Elaboración Propia

Para la creación de un registro DNS para las máquinas virtuales, el usuario deberá ubicarse en la hoja de configuración, hacer clic en la misma y especificar una etiqueta de nombre DNS único que luego se autocompletará con el dominio de Azure y guardar (Figura 88).

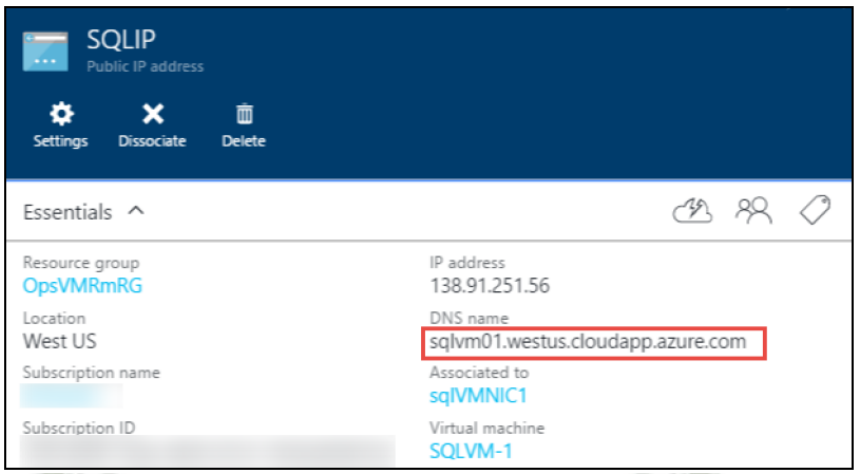
Figura 88: Configuraciones DNS



Fuente: Elaboración Propia

Después de que el nombre DNS se guarda copiar el nombre completo desde el panel de elementos esenciales de la dirección IP pública SQLIP (Figura 89).

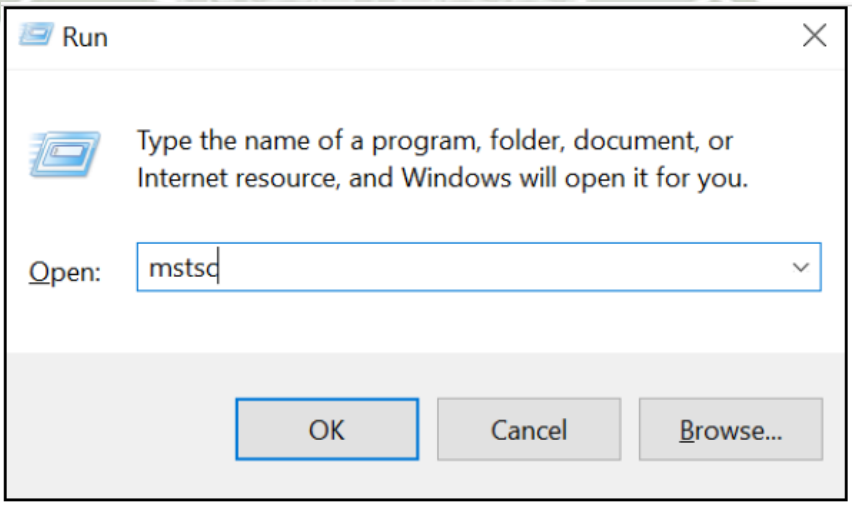
Figura 89: Características de IP pública.



Fuente: Elaboración Propia

Para que así se pueda conectar a la máquina virtual al ejecutar el cliente de escritorio remoto manualmente escribiendo mstsc en el cuadro de diálogo del ejecutar de Windows (Figura 90) y haciendo clic en aceptar.

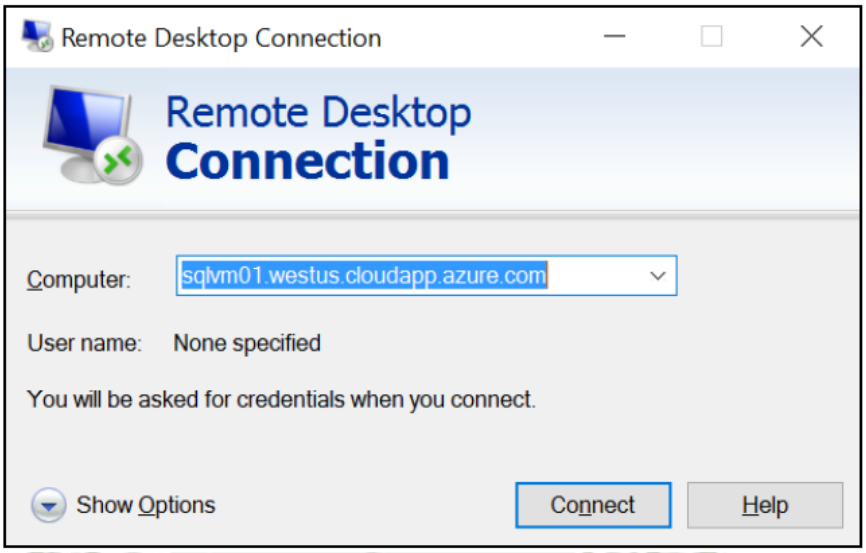
Figura 90: Ejecutar escritorio remoto.



Fuente: Elaboración Propia

Pegar el nombre DNS en el cuadro de diálogo de la conexión a escritorio remoto y hacer clic en conectar (Figura 91).

Figura 91: Conexión remota con dominio de Azure

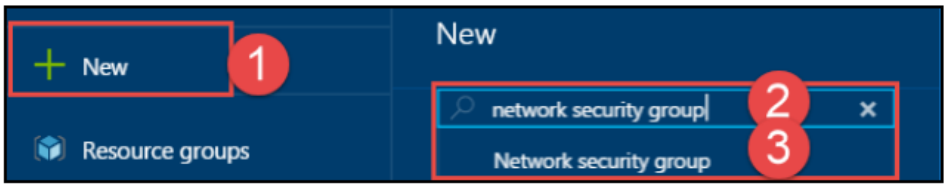


Fuente: Elaboración Propia

Después de haber comprobado que se puede conectar, desconectar la sesión cerrando el cliente de conexión a escritorio remoto (Figura 92).

Para crear un grupo de seguridad en la red haga clic en nuevo y, en el cuadro de texto de búsqueda digitar grupo de seguridad de red, y hacer clic en el resultado.

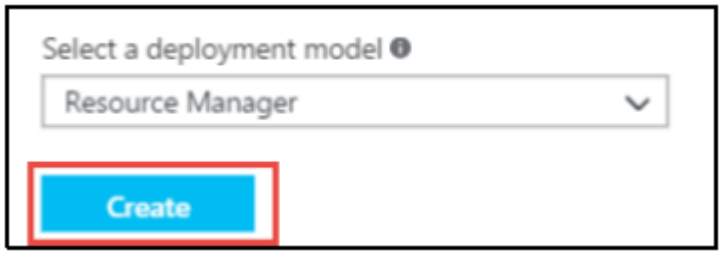
Figura 92: Creación de grupo de seguridad



Fuente: Elaboración Propia

Aceptar el administrador de recursos por defecto y hacer clic en crear.

Figura 93: Elección del administrador de recursos.

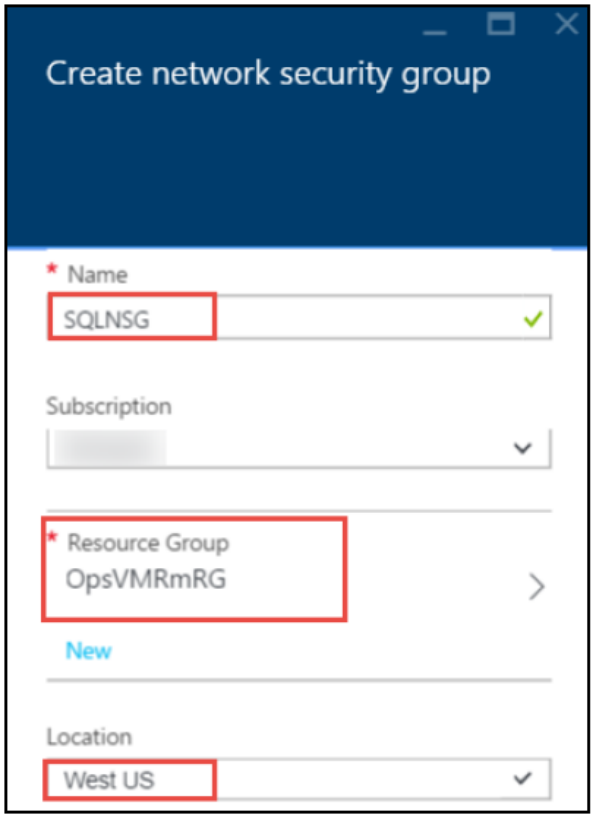


Fuente: Elaboración Propia

El usuario deberá especificar la siguiente configuración (Figura 94) en el cuadro de diálogo de la creación de grupo de seguridad de red:

a. Nombre: SQLNSG
b. Grupo de recursos: Seleccionar el grupo de recursos OpsVMRmRG existente.
c. Ubicación: Elegir la misma región que las máquinas virtuales.

Figura 94: Configuración de grupo de seguridad de redes.

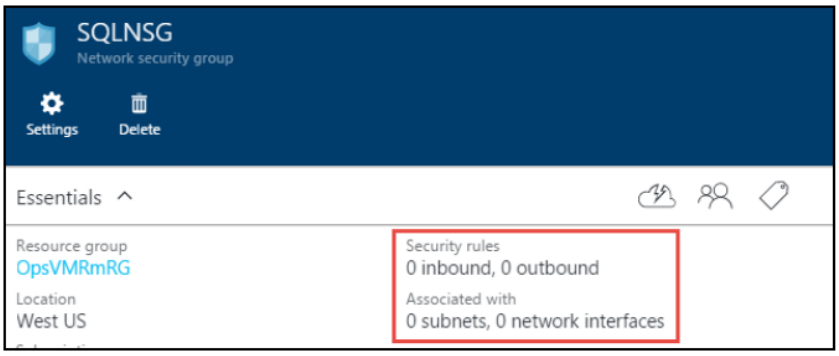


Fuente: Elaboración Propia

Hacer clic en crear después de que el grupo de seguridad de red está configurado.

Se debe tener en cuenta que el grupo de seguridad de red creado no está asociado con una interfaz de red o subred todavía, es decir que aún no hay una completa protección de los recursos (Figura 95).

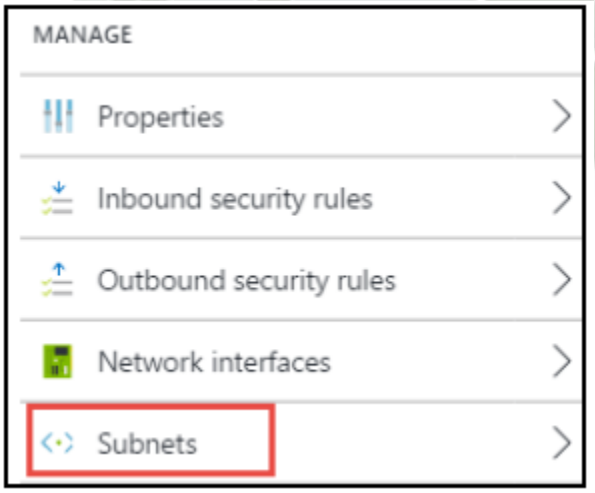
Figura 95: Grupo de seguridad de redes



Fuente: Elaboración Propia

Para poder asociar el grupo de recursos en una interfaz de red, el usuario deberá dirigirse a configuración de la lámina para el grupo de seguridad de red y hacer clic en subredes (Figura 96).

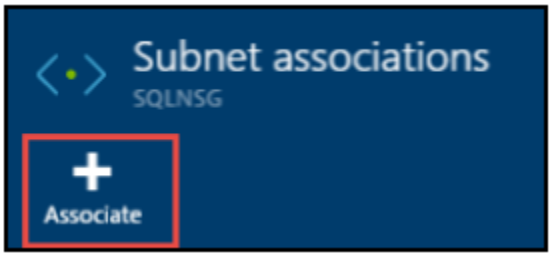
Figura 96: Opción de subredes



Fuente: Elaboración Propia

Hacer clic en el botón de asociado ubicado en la barra de herramientas.

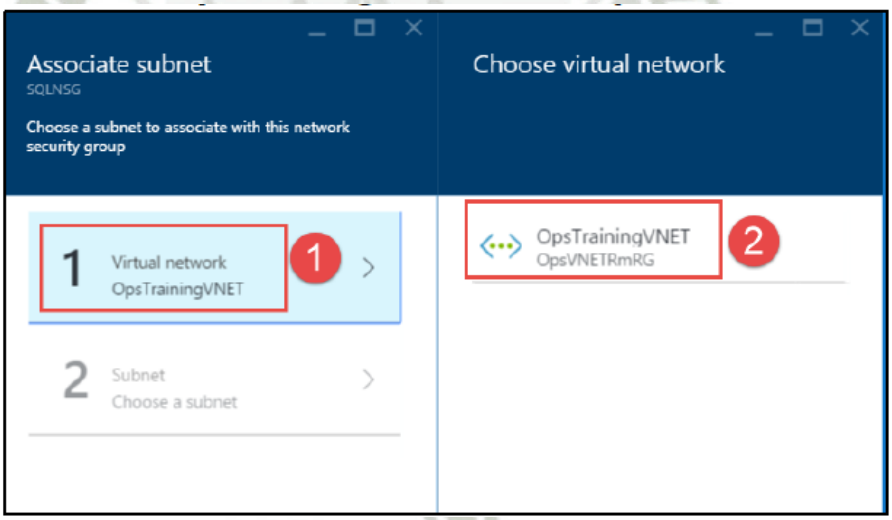
Figura 97: Asociar una subred



Fuente: Elaboración Propia

Seleccionar la red virtual, que este caso se llama OpsTrainingVNET y que se encuentra en el grupo de recursos OpsVNETRmRG.

Figura 98: Elección de red virtual.



Fuente: Elaboración Propia

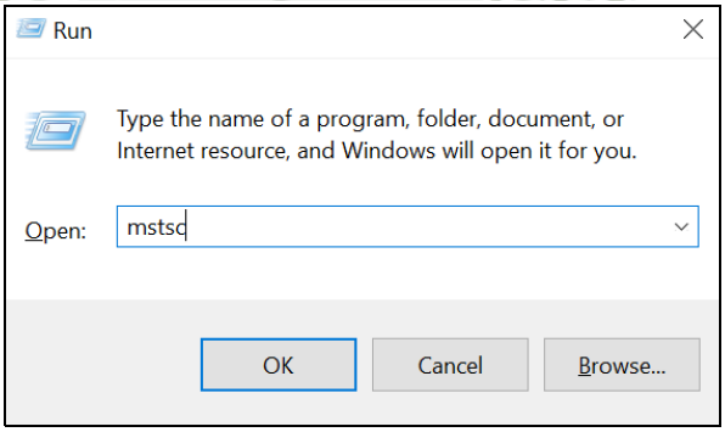
A continuación, seleccionar la subred de datos y hacer clic en aceptar (Figura 99) para que de esta manera la operación sea realizada correctamente en el grupo de seguridad de red y que las reglas puedan aplicarse a todo el tráfico de la subred.

Figura 99: Subred de datos.

Fuente: Elaboración Propia

El usuario deberá espere 1 - 2 minutos y luego Iniciar el cliente de escritorio remoto de nuevo escribiendo mstsc en el cuadro de diálogo Ejecutar de Windows (Figura 100) y haciendo clic en Aceptar.

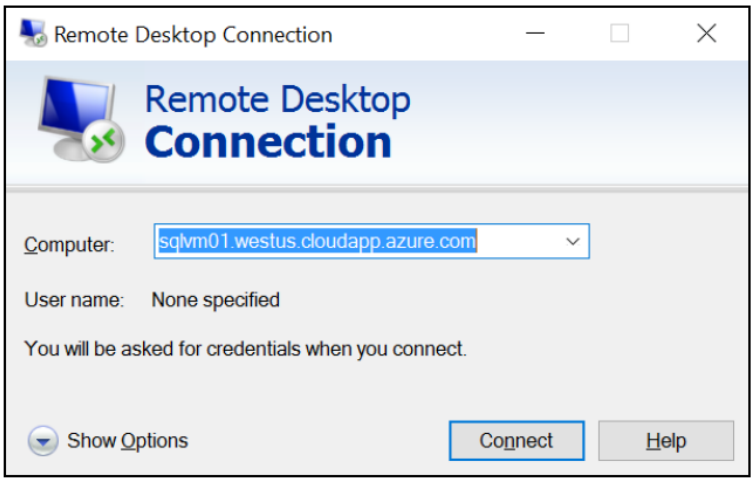
Figura 100: Ejecutar escritorio remoto.



Fuente: Elaboración Propia

Conectar con el mismo nombre DNS utilizado anteriormente. Esta vez, la conexión no debe tener éxito debido a las reglas predeterminadas del grupo de seguridad de la red (Figura 101).

Figura 101: Conexión remota con dominio de Azure.

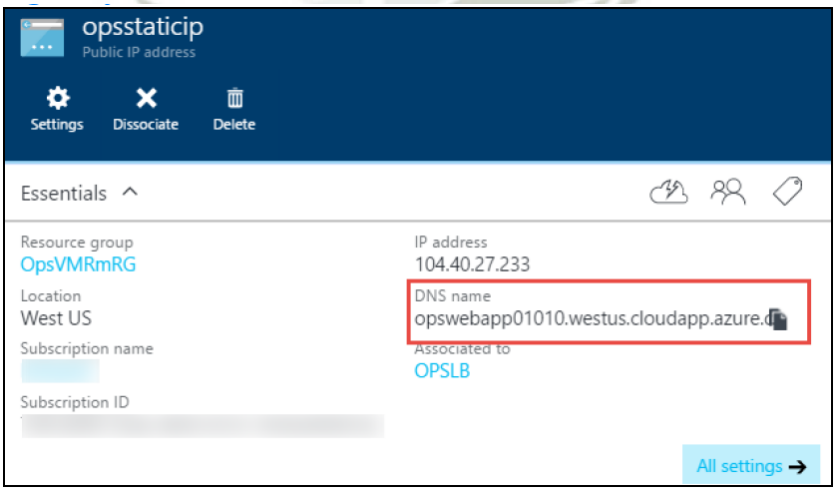


Fuente: Elaboración Propia

Para poder crear reglas de acceso se debe validar que la aplicación web sigue trabajando haciendo clic en Examinar, direcciones IP públicas, y la selección de la dirección IP pública opsstaticip (Figura 102).

Copia el valor para el nombre DNS, y pegarlo en una nueva instancia pestaña del navegador.

Figura 102: Nombre DNS brindado por Azure



Fuente: Elaboración Propia

Se debe esperar la carda del sitio web, esto significa que la conectividad a la base de datos todavía es producida dentro de la red virtual (Figura 103).

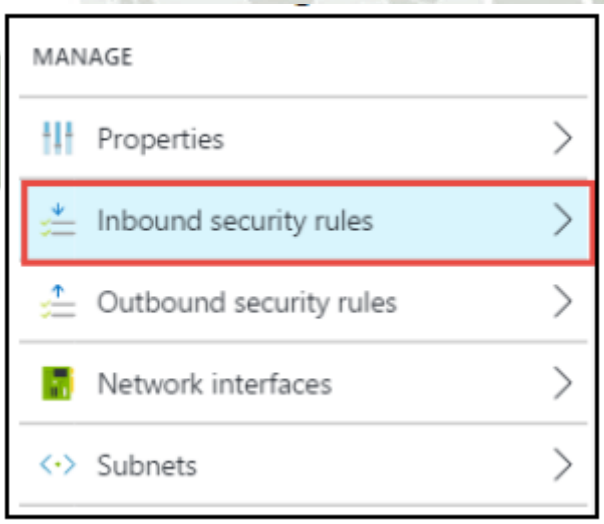
Figura 103: Estado de conectividad de la máquina virtual

Fuente: Elaboración Propia

El usuario deberá abrir el grupo de seguridad de la red SQLNSG nuevamente, haciendo clic en examinar, grupos de redes de seguridad, y la seleccionar SQLNSG usando el portal de administración de Azure.

En la configuración de la ventana hacer clic en reglas de seguridad entrante.

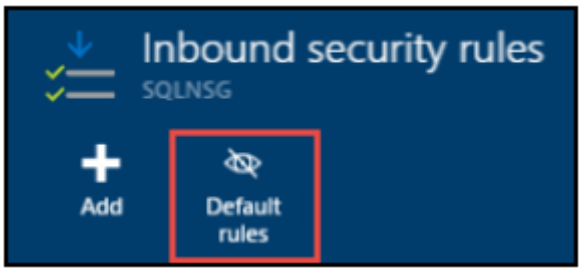
Figura 104: Ubicación de la opción para reglas de seguridad.



Fuente: Elaboración Propia

Se continúa haciendo clic en las reglas predeterminadas de la barra de herramientas (Figura 105).

Figura 105: Creación de reglas de seguridad.



Fuente: Elaboración Propia

Por defectos se encuentra tres tipos de reglas:

1. AllowVnetInBound: Es aquella reglas que permiten el tráfico desde cualquier dispositivo de la red virtual. Esto incluye todas las redes virtuales conectados o redes locales de en las instalaciones.
2. AllowAzureLoadBalancerInBound: Es aquella regla que permite el tráfico desde el equilibrador de carga. El SQLVM-1 tendría que ser parte de la configuración de la dorsal IP del equilibrador de carga para recibir el tráfico, pero por defecto, el GSN lo permitiría.
3. DenyAllInBound: Es aquella regla que es utilizada para el resto del tráfico denegado.

Figura 106: Listado de reglas de seguridad.

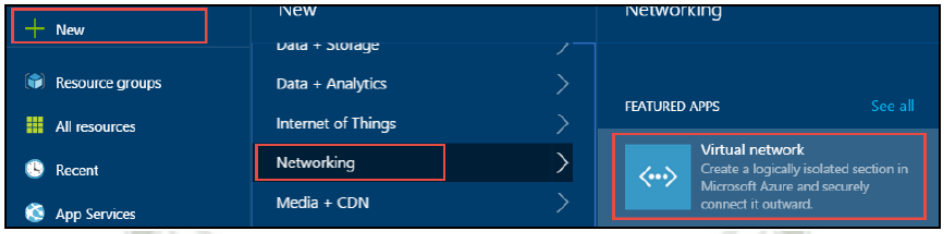
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	Any/Any	Allow	...
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	Any	Any/Any	Allow	...
65500	DenyAllInBound	Any	Any	Any/Any	Deny	...

```
Tip: Network security group rules are processed based on the priority.
Rules are processed based on the lowest priority rule first.
```

Fuente: Elaboración Propia

El usuario podrá crear una VPN, con los siguientes pasos. Se debe empezar creando una red virtual y para esto se debe hacer uso del portal de administración de Azure, hacer clic en nuevo, redes, y la red virtual (Figura 107).

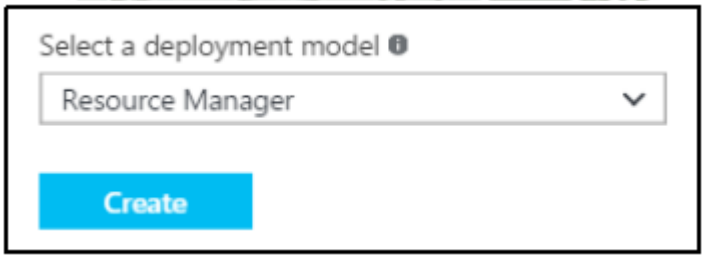
Figura 107: Creación de una red virtual.



Fuente: Elaboración Propia

Aceptar el valor por defecto del administrador de recursos y hacer clic en crear.

Figura 108: Administrador de recursos.



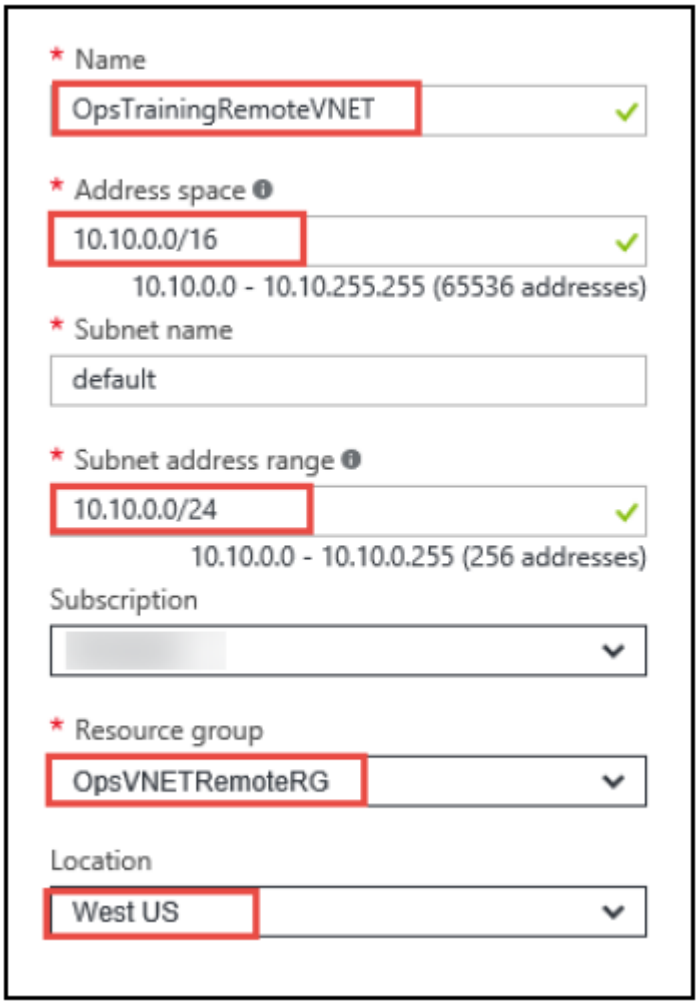
Fuente: Elaboración Propia

El usuario deberá especificar las siguientes configuraciones (Figura 109), respecto a su segmentación de red interna, en este caso utilizaremos el segmento de red 10.10.0.0:

- Nombre: OpsTrainingRemoteVNET
- Espacio de direcciones: 10.10.0.0/16
- Subred rango de direcciones: 10.10.0.0/24

- Suscripción: Elija su suscripción
- Grupo de recursos: OpsVNETRmRG
- Localización: Especificar una región remota de la región que está utilizando actualmente.

Figura 109: Configuraciones de red.

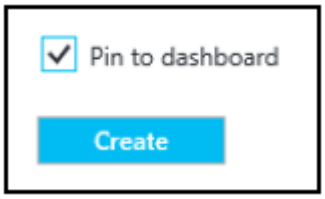


Fuente: Elaboración Propia

Se debe asegurar de que esta no es la misma ubicación que ha especificado en las sesiones anteriores.

Proceder con la comprobación de los terminales de tablero de instrumentos, y luego hacer clic en crear para la creación de una nueva red virtual (Figura 110).

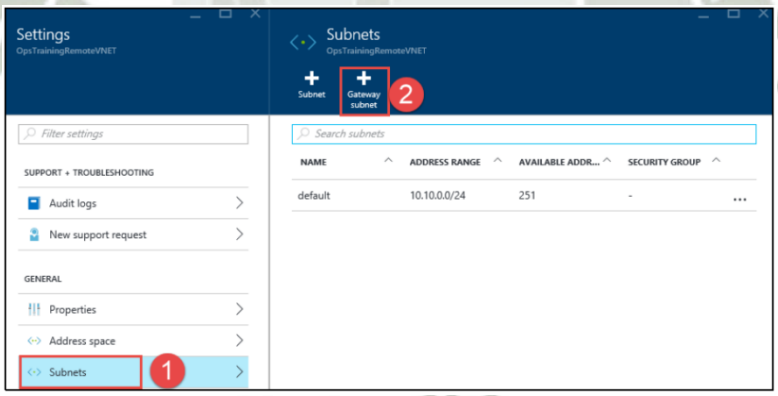
Figura 110: Comprobación de terminales de tablero de instrumentos



Fuente: Elaboración Propia

Para poder configurar una subred de entrada y salida para ambas redes virtuales se debe ir a la red virtual VNET dentro hoja de configuración OpsTraining, y hacer clic en subredes y en puerta de enlace de la subred (Figura 111).

Figura 111: Tipos de subredes.

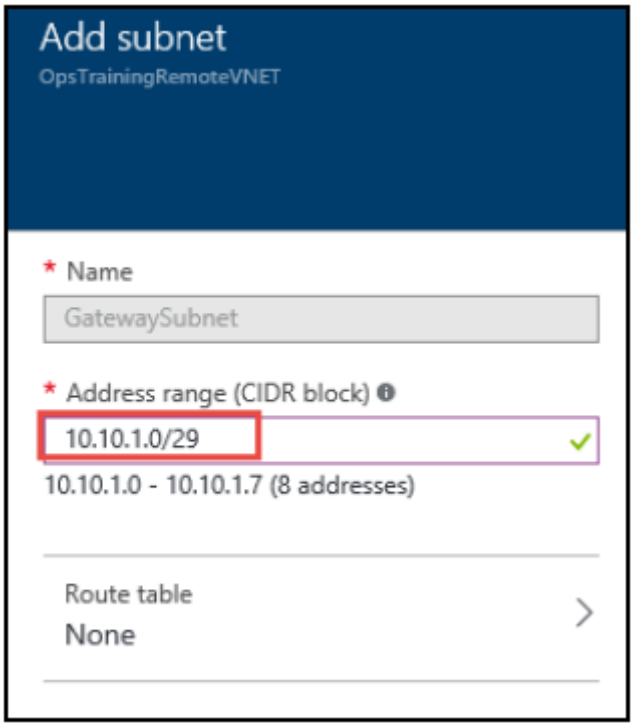


Fuente: Elaboración Propia

Especificare la siguiente configuración para la subred y hacer clic en OK.

- Nombre: GatewaySubnet
- Direccionamiento: 10.10.1.0/29

Figura 112: Creación de subred para la puerta de enlace N°1

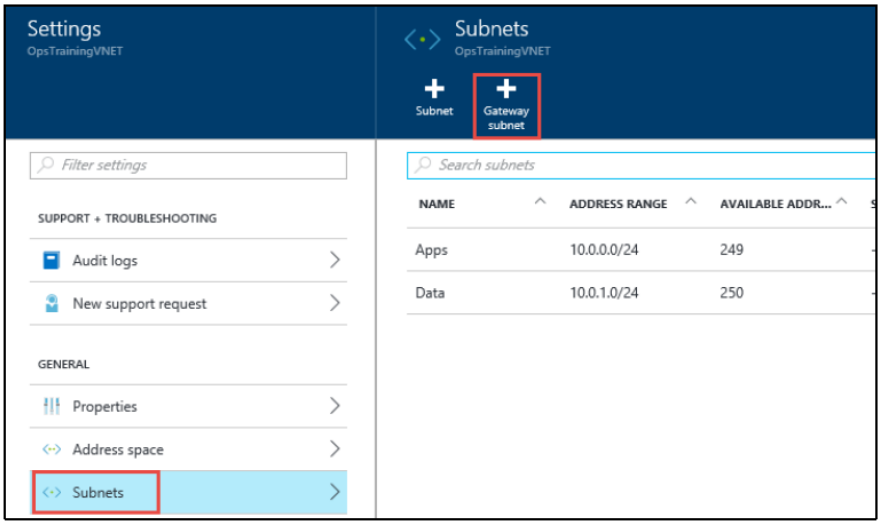


Fuente: Elaboración Propia

Abrir la hoja de configuración OpsTrainingVNET haciendo clic en examinar, redes virtuales, y luego hacer clic en OpsTrainingVNET.

En la hoja de configuración de red virtual OpsTrainingVNET, haga clic en subredes y haga clic en puerta de enlace de subred (Figura 113).

Figura 113: Tipo de subredes.

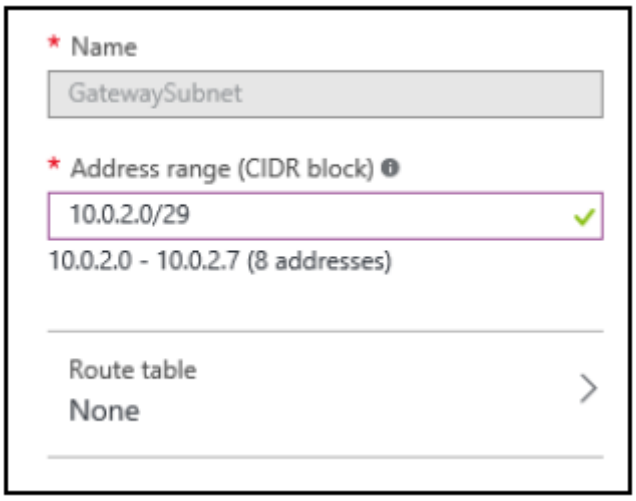


Fuente: Elaboración Propia

Especificar la siguiente configuración (Figura 114) y hacer clic en OK.

- Nombre: GatewaySubnet
- Direccionamiento: 10.0.2.0/29

Figura 114: Creación de subred para la puerta de enlace N°2

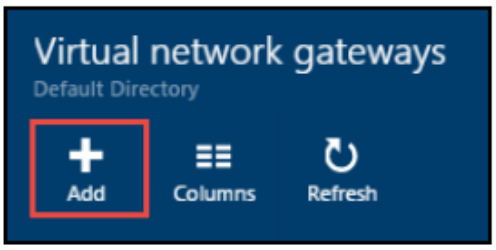


Fuente: Elaboración Propia

Para crear la primera puerta de enlace se debe hacer uso del portal de administración de Azure, hacer clic en examinar, puertas de enlace de red virtual.

Una vez hecho, hacer clic en el botón añadir en la barra de herramientas y colocar el nombre de la puerta de enlace que en este caso llamaremos OPSGW1

Figura 115: Agregar una puerta de enlace virtual N°1.



Fuente: Elaboración Propia

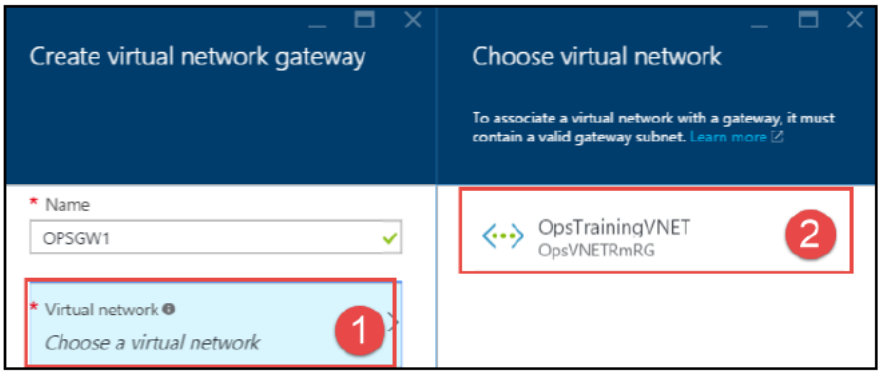
Seleccionar el grupo de recursos OpsVNETRmRG, y seleccionar la región de la formación de operaciones VNET donde se implementará (Figura 116).

Figura 116: Localización para la puerta de enlace virtual N°1

Fuente: Elaboración Propia

El usuario deberá hacer clic en la lista para elegir una baldosa de red virtual y seleccionar la formación de operaciones VNET (Figura 117).

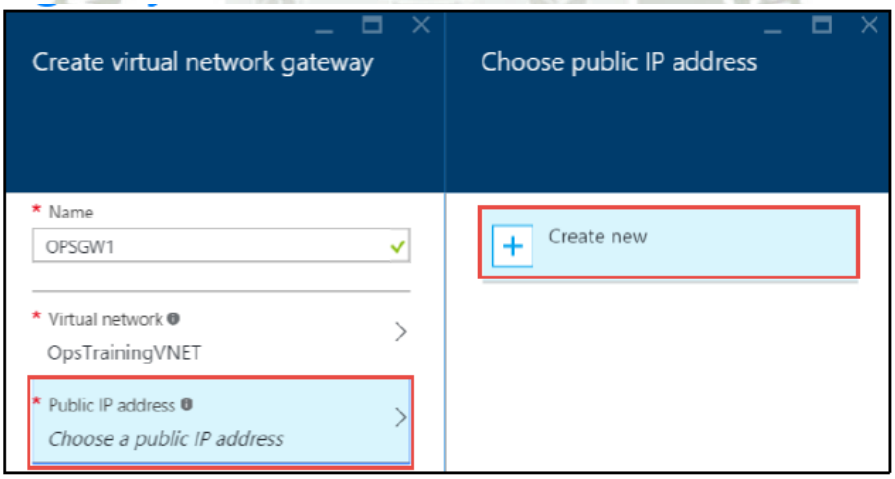
Figura 117: Selección de red virtual.



Fuente: Elaboración Propia

Hacer clic en el azulejo de la dirección IP pública y, hacer clic en crear nuevo. Ingresar el nombre, que en este caso será OPSGW1IP IP y hacer clic en OK.

Figura 118: Creación de IP Pública de la puerta de enlace virtual N°2.



Fuente: Elaboración Propia

En la parte inferior de la hoja hacer clic en crear para iniciar el aprovisionamiento de la puerta de enlace.

Para poder crear la segunda puerta de enlace se debe hacer uso del portal de administración de Azure, haga clic en examinar, puertas de enlace de red virtual.

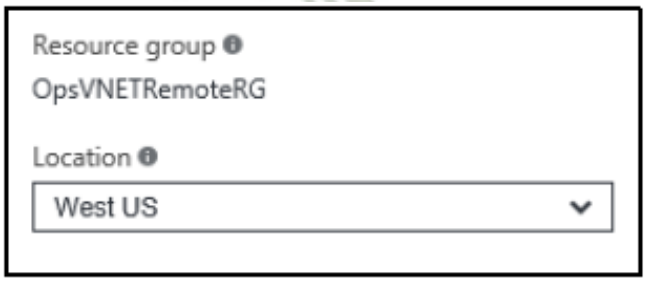
Hacer clic en el botón añadir en la barra de herramientas (Figura 119) y colocar el nombre de la puerta de enlace que en este caso llamaremos OPSGW2.

Figura 119: Agregar una puerta de enlace virtual N°2.

Fuente: Elaboración Propia

Seleccionar el grupo de recursos OpsVNETRmRG, y seleccionar la región del OpsTrainingRemoteVNET donde se implementará (Figura 120).

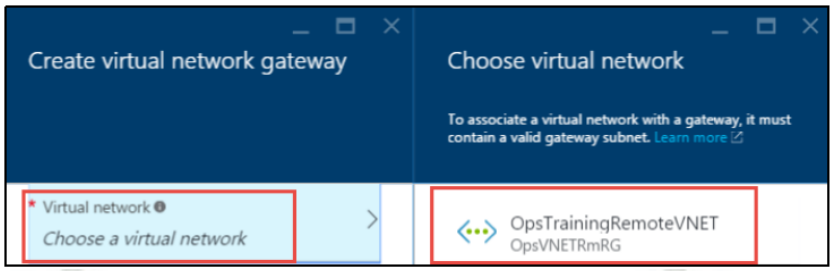
Figura 120: Localización para la puerta de enlace virtual N°2.



Fuente: Elaboración Propia

Hacer clic en la lista y elegir una baldosa de red virtual para así seleccionar OpsTrainingRemoteVNET (Figura 121).

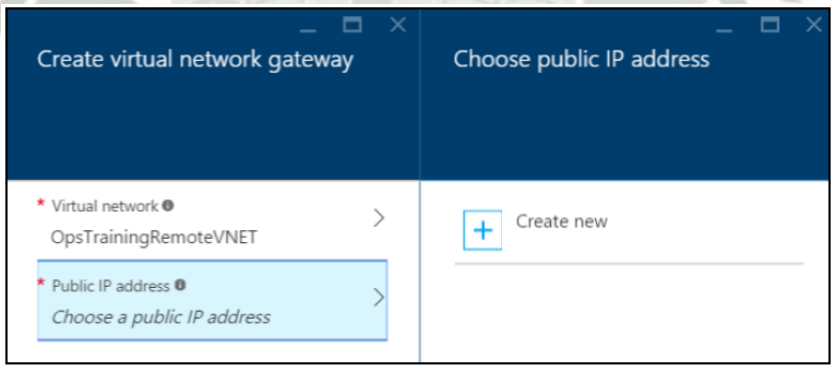
Figura 121: Selección de red virtual.



Fuente: Elaboración Propia

Hacer clic en el azulejo de la dirección IP pública y, hacer clic en crear nuevo. Ingresar el nombre, que en este caso será OPSGW2IP IP y hacer clic en OK (Figura 122).

Figura 122: Creación de IP Pública de la puerta de enlace virtual N°2.



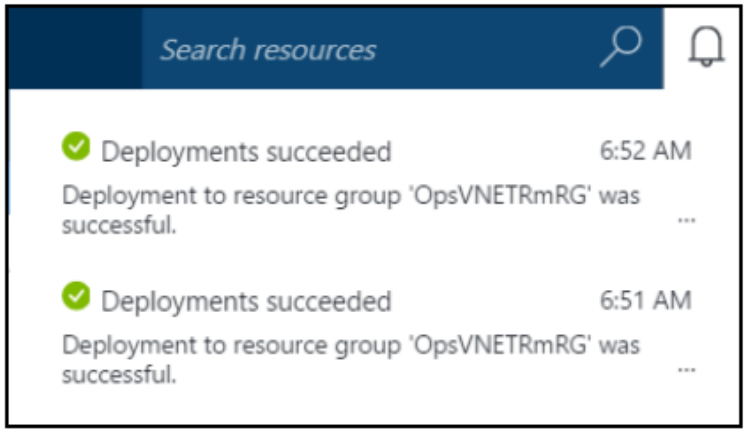
Fuente: Elaboración Propia

El usuario deberá hacer clic en el botón crear en la parte inferior de la hoja para iniciar el aprovisionamiento de la puerta de enlace (Figura 123).

Nota: Puede tardar hasta 60 minutos para la provisión de dos puertas de enlace.

El Portal Azure le notificará cuando los despliegues hayan completado.

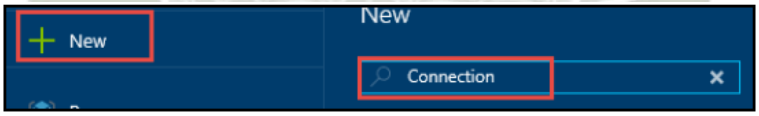
Figura 123: Registro del estado de actividad.



Fuente: Elaboración Propia

Para conectar las puertas de enlace de debe hacer uso del portal de administración de Azure, hacer clic en nuevo, y el tipo de conexión (Figura 124).

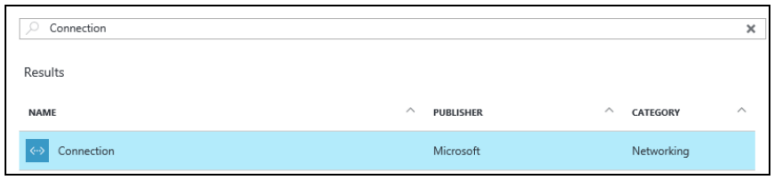
Figura 124: Buscador de componentes.



Fuente: Elaboración Propia

Hacer clic en conexión y, a continuación, hacer clic en crear (Figura 125).

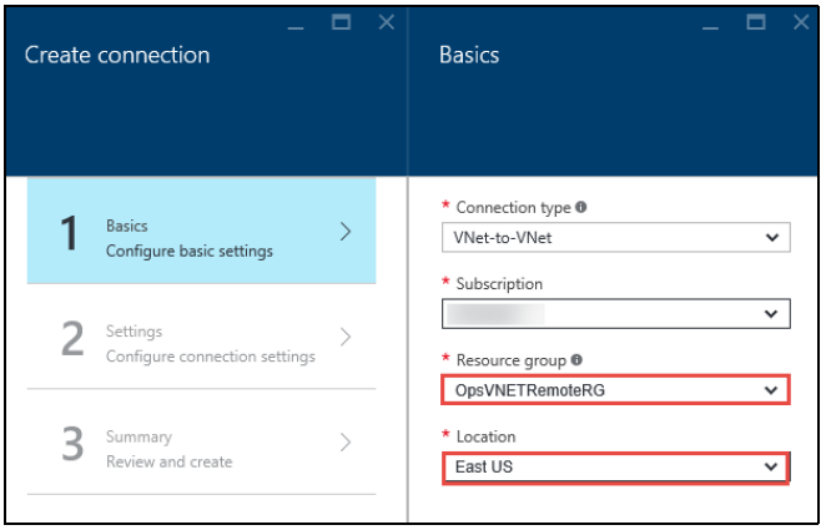
Figura 125: Icono para la creación de conexión.



Fuente: Elaboración Propia

Seleccionar el grupo de recursos existente OpsVMRmRG (Figura 126). A continuación, cambiar la ubicación de esta conexión con la región Azure de la red virtual en OpsTrainingVNET.

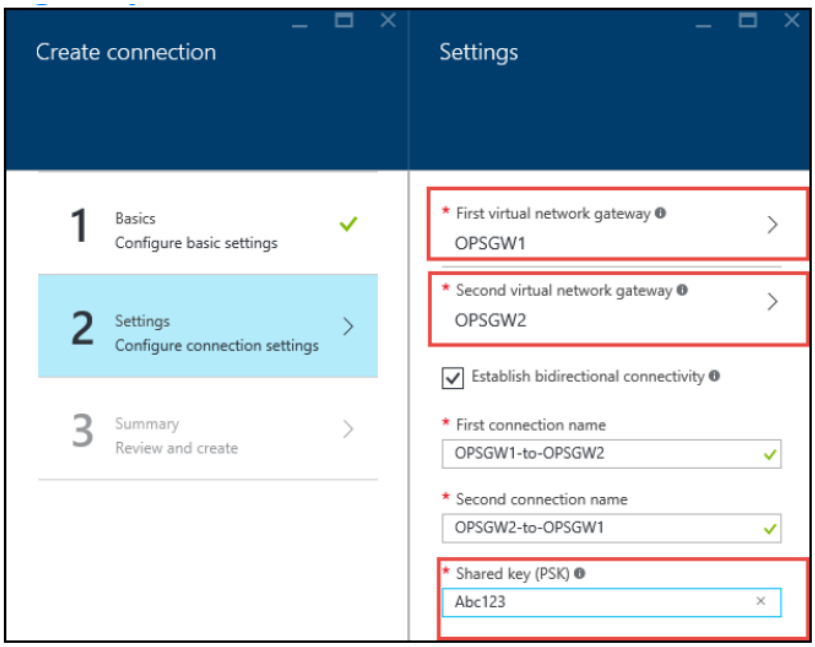
Figura 126: Especificaciones de conexión.



Fuente: Elaboración Propia

En la ficha de configuración (Figura 127), el usuario deberá seleccionar OPSGW1 por primera puerta de enlace de red virtual, y OPSGW2 para la segunda puerta de enlace de red virtual y hacer clic en OK.

Figura127: Ajustes de conexión.

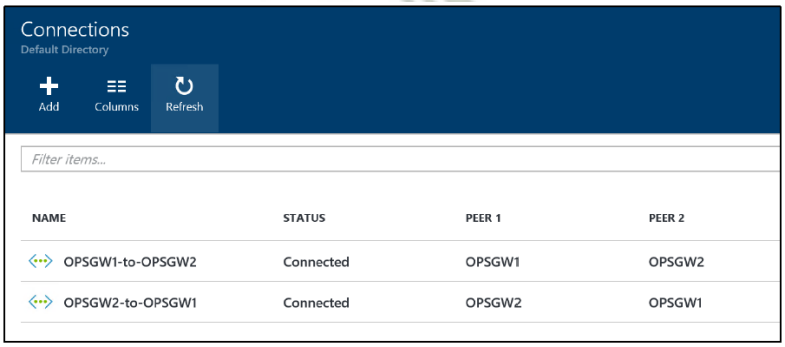


Fuente: Elaboración Propia

En la página de validación hacer clic en aceptar para poder crear la conexión.

Usando el portal de administración de Azure, hacer clic en examinar, conexiones (Figura 128). Ver el progreso del estado de la conexión y utilizar el icono actualizar hasta que cambie el estado de las conexiones de desconocido a conectado y se pueda asegurar que se logró establecer la conexión.

Figura 128: Lista de conexiones y su estado.



Fuente: Elaboración Propia.

Para poder validar la conectividad el usuario deberá crear una nueva máquina virtual en la segunda red virtual haciendo clic en nuevo, máquinas virtuales, y seleccionando el tipo Windows Server 2012 R2 Datacenter (Figura 129).

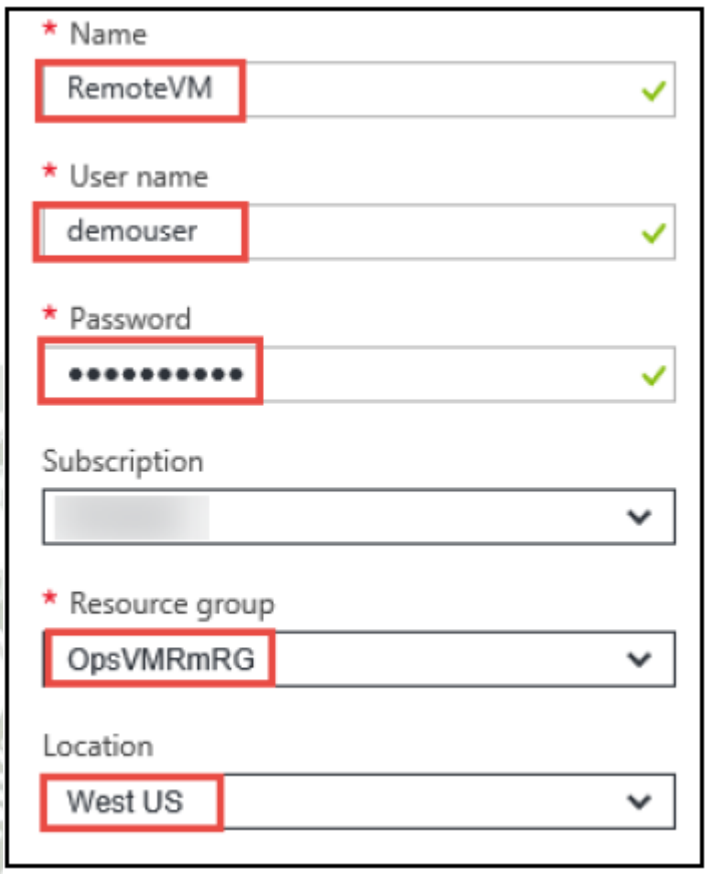
Figura 129: Opciones de sistemas operativos y los tipos de máquinas virtuales.

Fuente: Elaboración Propia

Especificar la siguiente configuración (Figura 130) y hacer clic en OK.

- Nombre: remotevm
- Nombre de usuario: demouser
- Contraseña: ****
- Grupo de recursos: OpsVMRmRG
- Localización: Se debe seleccionar la región donde se creó el OpsTrainingRemoteVNET red virtual.

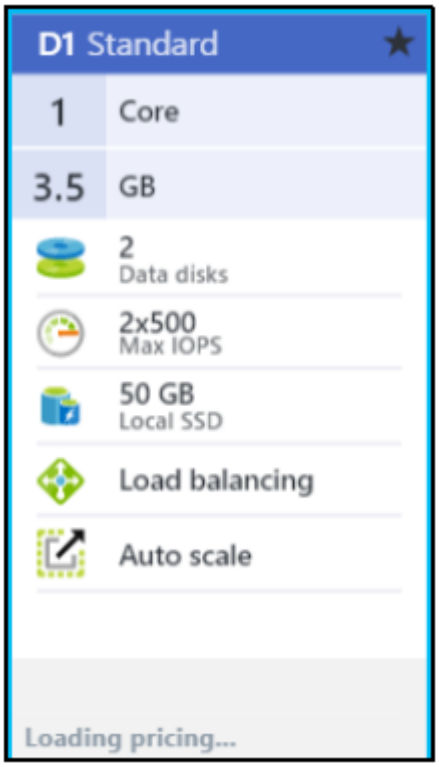
Figura 130: Especificaciones de creación para una máquina virtual.



Fuente: Elaboración Propia

Para las características del hardware, elegirla máquina virtual D1 estándar y seleccionar (Figura 131).

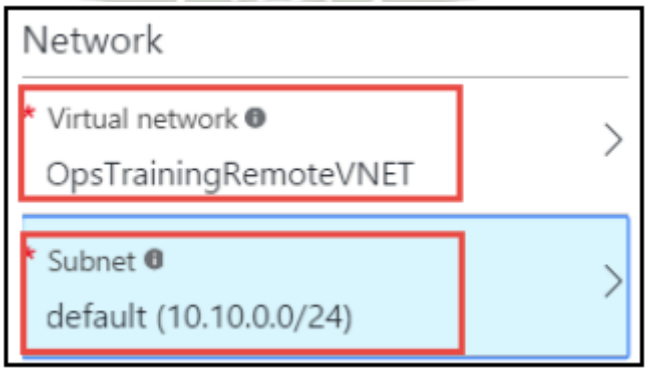
Figura 131: Características de hardware a elegir para una máquina virtual



Fuente: Elaboración Propia

En la hoja de configuración, cambiar la red virtual a OpsTrainingRemoteVNET, y establecer la subred a la subred predeterminada denominada: por defecto (Figura 132).

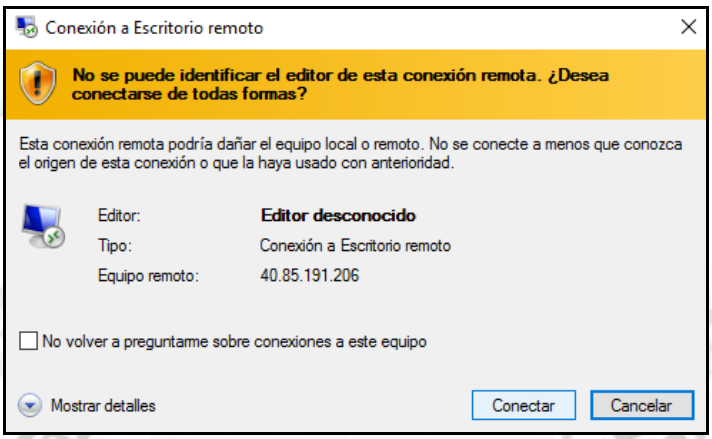
Figura 132: Red y distribución de subred.



Fuente: Elaboración Propia

Después de que la máquina virtual se aprovisiona puede validar la conectividad (Figura 133) a través del túnel VPN mediante la conexión usando el escritorio remoto (MSTSC) desde el interior de la máquina virtual WebVM-1 y conectarse a la IP privada de la máquina virtual RemoteVM.

Figura 133: Interfaz para la conexión remota.



Fuente: Elaboración Propia

Conclusiones

Después de la implementación, migración y pruebas del ambiente en alta disponibilidad alojado en la nube, se puede concluir los siguientes puntos.

1. Se agilizaron los procesos operativos internos con los servicios alojados en el ambiente de alta disponibilidad, del mismo modo se incrementó la seguridad con diferentes metodologías avanzadas de nivel empresarial que resguardan y garantizan la integridad de la información.
2. Se integraron de manera flexible los diferentes sistemas operativos, lenguajes de programación y diversas plataformas utilizados por la institución, el proceso de transición fue transparente y no se produjo incompatibilidad ni perdidas de información.
3. El diseño de la infraestructura y el incremento de un proxy gráfico fue óptimo en este proyecto ya que se pudo prevenir cualquier tipo de ataque que amenazaba con vulnerar la seguridad de la información organizacional.
4. Apostar por la adopción de nuevas tecnologías e incrementar el uso de ella, favorece al crecimiento empresarial al beneficiarse de las ventajas significativas que implican las comunicaciones en la nube, como es la escalabilidad, reducción de costos, mayor eficiencia, productividad y el incremento de flexibilidad.
5. Se obtuvieron los resultados esperados al favorecer a la correcta toma de decisiones empresariales y a la automatización de procesos con el fin de reducir recursos, todo esto fue logrado con el análisis de datos generados por los servicios con el uso de tecnologías de la información.

Recomendaciones

Dentro de las recomendaciones que planteo es dar un mayor impulso a la toma de decisiones acerca de la adopción de nuevas tecnologías en los diferentes ámbitos empresariales. Esto debido al elevado crecimiento y demanda de servicios directamente enlazados con la productividad de las compañías, que permiten prevenir y afrontar los nuevos retos tecnológicos. Además, es necesario contar con una infraestructura sólida en las oficinas de TI para los servicios con mayor concurrencia.

De acuerdo con un estudio de IDC (2016) se estimó que en este 2017 el mercado cloud crecerá un 36.6 % respecto al 2016 y alcanzará un valor aproximado de 152 millones de dólares al cierre del año, colocando como principal inversión la consideración de escenarios de infraestructura en la nube.

Dentro de las características que buscan las empresas, se encuentra la velocidad de respuesta ante las solicitudes y el respaldo de la información, y lo que se propone es reducir los tiempos de respuesta a través de la integración de zonas de dominio.

Para complementar el proyecto y optimizar más aún los tiempos de respuesta es necesario como una buena práctica migrar a la misma nube las zonas y registros DNS para que su actualización sea prácticamente instantánea.

Un objetivo a corto plazo del proyecto es la consideración para la transformación e implementación de servidores IaaS al servicio de plataforma (PaaS) que permitirá y aportará al desarrollo de aplicaciones y servicios empresariales, ya que cuenta con multi instancias por roles integrados en cloud service que permite el uso de diferentes servicios (almacenamiento, SQL, Visual

Studio), y conectividad directa con las redes virtuales. Para así facilitar el cambio de ambiente de desarrollo a producción.

Otra de las características que se trabajará en el futuro es la inclusión de inteligencia de negocios dentro de este escenario para poder trabajar la gestión de la información de una manera más óptima, utilizando inteligencia artificial para la gestión de información a través de servicios cognitivos que permitirán un análisis de comportamiento más detallado a través de la data generada por aplicativo o servicio. De esta manera se podrá garantizar una mejor experiencia para el usuario y una manera más avanzada para el proceso de gestión de los datos, los cuales serán almacenados en un storage diferente al de la solución brindada por Azure.

Por último, se desea implementar un bot de respuestas automatizadas para el portal web de la institución para facilitar la interacción del usuario y apoyar a una búsqueda más objetiva de la información a la que se acude respecto a documentación de los proyectos de inversión sostenible llevados por la entidad.

Se recomienda implementar las funcionalidades de Active Directory en la nube para la correcta conexión de todos los servicios alojados en la nube, dentro de un servidor que cumpla con el rol de administrador y puedan interconectarse con todos las máquinas virtualizadas en la plataforma.

Referencias Bibliográficas

Beaty, Shaikh & Watson. (2009). Cloud Transformation Planning, presented at the Parallel & Distributed Processing. IBM New York, USA.

IBM Corporation. (2010). Cloud Services. Retrieved 17 May, 2010, from ftp://ftp.software.ibm.com/la/documents/imc/la/ar/mendoza/movilidad_web_20_y_cloud_computing_hechos_simples.

Wozniak, T. (2010). Grid and Cloud Computing, A Business Perspective on Technology and Applications, Primera ed. Berlin Heidelberg.

Azure. (2016). Windows Azure. Retrieved 20 April, 2016, from http://www.microsoft.com/windowsazure. 2016.

Customer Proprietary Network Information. (2010). Cloud Computing and Information Security Briefing.

NIST. (2010). Special Publication 800145. The NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/publications/nistpubs/ 800145/SP800145.

Ferris & Farrell. (2003). Ferris C, Farrell J. – IBM Research Triangle Park, What are Web Services? Association for Computing Machinery - ACM Digital Library. Retrieved from: http://portal.acm.org/citation.cfm?id=777335. 2003.

Murazzo, Segura & Villafañe. (2010). Murazzo, Segura y Villafañe, Cloud Computing Con Windows Azure. Tema desarrollado en la segunda Jornada de Actualización Informática.

Carroll, Merwe & Kotze. (2011). Carroll, M., A. van de Merwe, and P. Kotze. Secure Cloud Computing: Benefits, Risks and Controls, In Proceedings of the Information Security. South Africa, pp. 19.

Rodríguez, Murazzo & Di Sciacio. (2011). Nelson R. Rodríguez, María A. Murazzo, Cecilia di Sciacio. Integración de Computación móvil con Cloud Computing. 1º Seminario Argentina Brasil de Tecnologías de la Información y la Computación; bajo el lema "Las TIC como oportunidad de integración".

Parthipan, Sriprasadh & Maheshkumar. (2013). Parthipan, Sriprasadh, Maheshkumar. Secure Information Transaction In Hybrid Cloud Computing. Information Communication and Embedded Systems (ICICES).

Hernández. (2011). Hernández Ramírez. Sistema de almacenamiento de archivos con tolerancia a fallos utilizando Cloud Híbrido. Tesis de Maestría en Computación. Victoria, Tamaulipas, México.

Yousaf et al., (2013). Yousaf Saeed, ATahir, S Mughal, M.Khan. Insight into Security Challenges for Cloud Databases and Data Protection Techniques for Building Trust in Cloud Computing. Journal of Basic and AppliedScientific Research.