# **PROYECTO DE AZ-104:**

# **ESTRUCTURA ON PREMISES, NUBE HIBRIDA Y NUBE PÚBLICA**

El objeto de este proyecto consiste en hacer la migración de los equipos y servicios de una oficina a la nube de Azure.

Partimos de una estructura on-premises como se ve en el siguiente esquema:



**Parte1: Simular en vmWare la estructura on-premises**

**1: Carga de los equipos**

Simulad la red on-premises del esquema en vmWare.

La simulación estará compuesta por los siguientes seis equipos:

**Rou100**: Tiene la misión de permitir comunicar las redes internas con internet. Está formada a partir de un Linux Debian configurado para dar los servicios de enrutamiento entre la red 100 e internet y de DHCP en la red 100.

**pfSense**: Es un firewall que permite el tráfico entre la red 10 e internet, publica un servicio web del equipo IIS en su IP pública y proporciona el servicio de DHCP a la red 10.

**WS22**: Es un Windows Server 2022. Proporciona servicios de directorio activo, DNS y ficheros compartidos.

**W11-01**: es un Windows 11 23H2 (puede ser el lyte), agregado a dominio del servidor WS22

**IIS**: Es un equipo con Windows Server 2022 con el rol de servidor de IIS, publicando una página web.

**PCCasa01**: Equipo con Windows 11 23H2 simulando estar en una red doméstica.

**Rou11**: Simula un router doméstico. Proporciona enrutamiento entre la red doméstica e internet y servicio de DHCP en la red 11.

**2: Configurar el equipo IIS**

Instalad un Windows server 2022. Proporcionad la siguiente configuración:

No pertenece a ningún dominio

Está conectado en vmNet12, con la dirección IP 192.168.12.2/24 con 192.168.12.1 como puerta de enlace predeterminada.

Tiene el rol de Servidor de IIS. Colocad alguna página web estática para que la sirva el IIS, que no sea la página que trae por defecto.

**3: Configurar equipo W11-01**

Arrancad el equipo Rou100

Conectad el equipo a la vmNet10

Actualizad Windows

Cargad la versión 7.x de PowerShell

Cargad Azure CLI

Cargad el módulo de Azure para PowerShell

Probad que se puede conectar a vuestro tenant tanto desde el CLI (az login) como desde PowerShell (Connect-AzAccount)

Cambiad la red virtual de la máquina a vmNet10

**4: Configurar el equipo pfSense**

Configurad el equipo con 3 adaptadores (WAN, LAN y DMZ) con las direcciones IP del esquema.

Configurad el servicio de DHCP en la red interna.

Continuad la configuración de este equipo desde W11-01.

Modificad el servicio de DHCP para que proporcione, como configuración de servidor DNS, la dirección 192.168.10.2 y de dominio por defecto msm.loc.

Publicad, en su adaptador WAN, la página web servida por el equipo IIS.

Comprobad que W11-01 puede acceder a internet (no necesariamente navegar) y a la web publicada en la WAN del pfSense.

Preparad el servicio de OpenVPN y generad los ficheros necesarios para que, más adelante, PCCasa01 pueda conectarse a la red mediante OpenVPN.

**5: Red doméstica**

Configurad el equipo Rou11 para que se pueda enrutar desde la red vmNet11 y hacia la red vmNet4.

Tiene que proporcionar servicios de DHCP, utilizando como servidores de DNS los de Google.

Cargad el equipo PCCasa01 como un clon lincado de W11-01. Aseguraos de modificar su MAC y su Windows ID.

Conectad el equipo PCCasa01 con la red vmNet10 utilizando el equipo pfSense mediante una conexión VPN point-to-site.

Comprobad que se puede hacer ping entre PCCasa01 y W11-01 en los dos sentidos.

Dad de alta el equipo en el dominio.

**6: Servidor de dominio**

Cargad el equipo WS22 mediante un clon lincado de la máquina IIS. Aseguraos de modificar su MAC y su Windows ID.

Configurad la IP según el esquema y poned de servidores de DNS los de Google.

Comprobad que el equipo puede navegar y actualizad Windows.

Promocionad el equipo a servidor de dominio (del dominio msm.loc) y servidor de DNS.

Agregad al dominio la máquina W11-01.

En el AD cread los siguientes grupos de seguridad:

* Depto1
* Depto2
* Depto3

Y los siguientes usuarios:

* Usu11 (miembro de Depto1)
* Usu12 (miembro de Depto1)
* Usu21 (miembro de Depto2)
* Usu22 (miembro de Depto2)
* Usu31 (miembro de Depto3)
* Usu32 (miembro de Depto3)

Cread una carpeta en “c:\” con el nombre de “Datos”

En esta carpeta debe tener los siguientes permisos:

* Administradores rwe
* Depto1 rxe
* Depto2 rxe
* Depto3 rxe

Cread una carpeta en “c:\Datos” tres carpetas con los nombres “D1”, “D2”, “D3” y “Temp”, con los siguientes permisos:

* En D1, los Administradores rwe y Depto1 rxe
* En D2, los Administradores rwe y Depto2 rxe
* En D3, los Administradores rwe y Depto3 rxe
* En Temp, los Administradores, Depto1, Depto2 y Depto3 rwe

Dentro de “C:\Datos\D1” crearemos tres carpetas: U1, U2 y Com, con los siguientes permisos:

* En U1, los Administradores y Usu11 rwe
* En U2, los Administradores y Usu12 rwe
* En Com, los Administradores y Depto1 rwe

Dentro de “C:\Datos\D2” crearemos tres carpetas: U1, U2 y Com, con los siguientes permisos:

* En U1, los Administradores y Usu21 rwe
* En U2, los Administradores y Usu22 rwe
* En Com, los Administradores y Depto2 rwe

Dentro de “C:\Datos\D3” crearemos tres carpetas: U1, U2 y Com, con los siguientes permisos:

* En U1, los Administradores y Usu31 rwe
* En U2, los Administradores y Usu32 rwe
* En Com, los Administradores y Depto3 rwe

Compartid la carpeta “C:\Datos”.

Estableced una política que mapee “C:\Datos” en la unidad Z de todos los equipos con Windows 11 del dominio.

Desde los equipos W11-01 y PCCasa01, abrid sesión con los usuarios Usu11, Usu21 y Usu31 y comprobad que tienen mapeada la unidad Z y que, en ella, pueden acceder y crear documentos solo en sus respectivas carpetas y departamentos.

**Parte 2: Migrar a nube híbrida**

**1: Migrar el servicio WEB**

Migrad el servicio de páginas web a Azure. Realizad una comparativa de las ventajas e inconvenientes de migrar a una plataforma IaaS o a una PaaS. Cuantas más opciones diferentes se propongan, mejor estará realizado el estudio.

En la que se haya comprobado que es más interesante, subid la página web y comprobad que es accesible desde WS22, W11-01 y PCCasa01.

Modificad lo necesario para que estos equipos puedan acceder a la página web utilizando el nombre [www.msm.loc](http://www.msm.loc) desde sus respectivos navegadores.

Cuando funcione correctamente, apagad el equipo IIS y configurad el equipo pfSense para que no publique ningún servicio web y, luego, desconectadle el adaptador que tiene en la DMZ. Tiene que terminar siendo un firewall sin DMZ (con solo zona roja y verde)

**2: Conectad la red on premises con la red de Azure**

Desactivad de PCCasa01 el adaptador OpenVPN que utilizaba para conectarse a vmNet10 y estableced una conexión point-to-site VPN con la red de Azure. Comprobad que este equipo sigue teniendo acceso a la unidad Z o realizad las operaciones necesarias para que lo haga.

Sustituid el equipo pfSense por un Windows server 2022 con dos adaptadores de red. Para esto, reutilizad la máquina IIS, conectando su adaptador de red a vmNet10 y agregándole un nuevo adaptador de red conectado a la vmNet4. Quitadle el rol de servidor de IIS y renombrad la máquina a WSVPN. Activad en este equipo el rol de servidor DHCP con la misma configuración que tenía el pfSense.

Montad una conexión VPN Site-to-site entre la red on premises vmNet10 y la red de Azure. Utilizad para hacerlo el “servicio de acceso remoto y enrutamiento” del equipo WSVPN.

Una vez conectados con las dos VPN, comprobad que todos pueden seguir navegando por Internet.

**3: Sincronización de usuarios**

Realizad las operaciones necesarias para sincronizar los usuarios y grupos de Windows Active Directory con nuestro tenant de Azure Active Directory.

**Nota:** solo sincronizad los usuarios y grupos de nuestro ejercicio, incluido el administrator y el grupo administrators. No los creados por defecto en Windows Server.

Cread una máquina virtual de Windows 11 en Azure con el nombre AW11. Haced que se pueda abrir sesión en ella con cualquiera de los usuarios que acabamos de sincronizar.

**4: Sincronización de carpetas**

Realizad lo necesario para sincronizar la carpeta C:\Datos del servidor WS22 con un almacenamiento del tipo file-share en Azure.

Cread varios ficheros de prueba en ambos sitios y aseguraos de que se replican en el otro.

Comprobad, desde los equipos W11-01 y PCCasa01 que pueden acceder tanto a los ficheros del servidor WS22 como a los replicados en Azure.

Realizad las operaciones necesarias para mantener los mismos permisos de ficheros y carpetas que tenían on premises.

**5: Migrar el servicio de archivos compartidos**

Modificar la política del servidor para que, en los clientes, se monte la unidad Z utilizando la carpeta compartida de Azure en lugar de la on premises.

Quitad del AD local los equipos W11-01 y PCCasa01 y agregadlos al directorio activo de Azure

Desmontad la sincronización de carpetas y archivos entre WS22 y la nube.

Modificad los servicios de DHCP del WSVPN y del router doméstico para hacer que, el servidor de DNS que proporcionen a sus clientes de DHCP, sean los de Google.

Llegados a este punto, apagad el servidor WS22 y aseguraos de que todo sigue funcionando.

**Parte 3: Trabajar en la nube pública**

En este momento, tenemos en la oficina el equipo WSVPN para encargarse de las comunicaciones y del servicio DHCP. Y, el resto de las máquinas (el equipo W11-01) serían los equipos de oficina que estarían trabajando sin servidores on premises.

Los equipos remotos se conectan directamente a Azure, sin solicitar ningún servicio a la oficina.

Todos los servicios estarían en la nube, con lo que ya no trabajamos con una nube hibrida si no con una nube pública.

**1: Realizar copias de seguridad en la nube**

Nuestro objetivo es realizar todos los días, a las 10 de la noche, una copia de seguridad de los datos que tenemos en el almacén de ficheros compartidos. Estas copias se guardarán durante 30 días. Las copias realizadas el día 1 de cada mes, se guardarán durante un año. Y las copias que se realicen el día 1 de enero, se guardarán durante 10.

Para nuestra práctica, empezaremos mandando realizar al momento una copia de seguridad de los ficheros y carpetas compartidas. A continuación, borraremos la carpeta de un usuario y realizaremos las operaciones necesarias para restaurarla utilizando la copia de seguridad recién realizada.

**2: Monitorizar el uso de la red y recursos**

Configurad una consola que nos permita ver el uso que estamos realizando de la red, de los recursos de almacenamiento de ficheros compartidos y del servidor web. Monitorizad también el uso de la máquina virtual que creamos en Azure.

Simulad, desde alguno de los equipos on premises, operaciones que puedan implicar uso de esos recursos (por ejemplo, subir un fichero grande a la carpeta compartida y luego borrarlo. Tened en cuenta que el tráfico de subida es gratis) y comprobad como el monitor lo refleja.

**3: Uso de computación en la nube**

Abrid sesión de escritorio remoto desde la máquina W11-01 a la máquina AW11, utilizando el mismo usuario de AD que utilizamos para acceder en local.

Mapead, en la máquina de Azure, una unidad Z igual a la que tenemos on premises. Comprobad que todo sigue funcionando como lo hacía en la máquina W11-01.

Cargad en la máquina virtual de Azure algún software de cliente (por ejemplo, WinRar, NotePad++, Acrobat Reader, etc.) y comprobad que podemos trabajar desde esta máquina como antes lo hacíamos en on premises.

Llegados a este punto, podríamos desmapear la unidad Z del equipo W11-01.

A partir de ahora, el usuario de oficina que utilizaba este equipo puede acceder a todo lo que utiliza en la oficina desde cualquier equipo con acceso a internet que soporte un cliente RDP, independientemente del operativo utilizado (Windows, Linux, MacOS, Android, etc.) y desde cualquier sitio del mundo.

**4: Servicio de escritorio remoto de Azure**

Analizad, sin implementarlo, la posibilidad de hacer lo mismo que acabamos de hacer en el punto 3, pero utilizando el servicio de escritorio remoto de Azure (Azure Virtual Desktop).

Estudiad los costes por equipo de utilizar esta solución y las ventajas e inconvenientes frente al uso de la máquina virtual anterior.

**5: Gobernanza de Azure**

Estudiad la posibilidad de bloquear, mediante directivas, a los usuarios de los grupos Depto1, Depto2 y Depto3, que puedan hacer login en ninguna máquina virtual fuera del horario de 8:00 a 15:00.

Facilitad, mediante roles RBAC, que el usuario Administrator, traído desde on premises, pueda crear máquinas virtuales en el grupo de recursos que hemos utilizado para está práctica. Abrid una ventana de navegador en incógnito y abrid sesión en el portal utilizando el usuario Administrator. Comprobad que puede crear y borrar una máquina virtual.

**6: Análisis de costos de la migración a Azure**

Supongamos que nuestra estructura inicial on premises, con una estructura de red similar a la del esquema inicial de este proyecto, estuviera compuesta por de 50 puestos de usuario con Windows 10 y dos servidores Windows 2012R2 en la oficina, y 25 usuarios móviles (Road Warriors) también con Windows 10.

Pretendemos pasar todos equipos de cliente a Windows 11 y, para poder hacerlo, necesitamos renovar 30 de los equipos. Los dos servidores también queremos renovarlos y que los nuevos utilicen Windows Server 2022.

Queremos estudiar la posibilidad de mantener nuestros equipos de cliente como están y utilizarlos para acceder a equipos de escritorio remoto en la nube de Azure. Y los servicios de los servidores pasarlos también a Azure, apagar los servidores locales y deshacernos de ellos.

Utilizando la calculadora de costo total (TCO) de Azure, Realizad un estudio económico de la rentabilidad de hacer estos cambios y recomendar la mejor solución a la dirección de la empresa.