Avance 1 del proyecto (Red Team vs Blue Team en Azure)

Integrantes:

Betzabeth Araya Abarca

Jose Arias Rodríguez

Carlos Garreta Quesada

Luis Ugalde Álvarez

Jose Ugalde Moreno

Fiorella Ureña Jaubert

Curso: Programación Avanzada

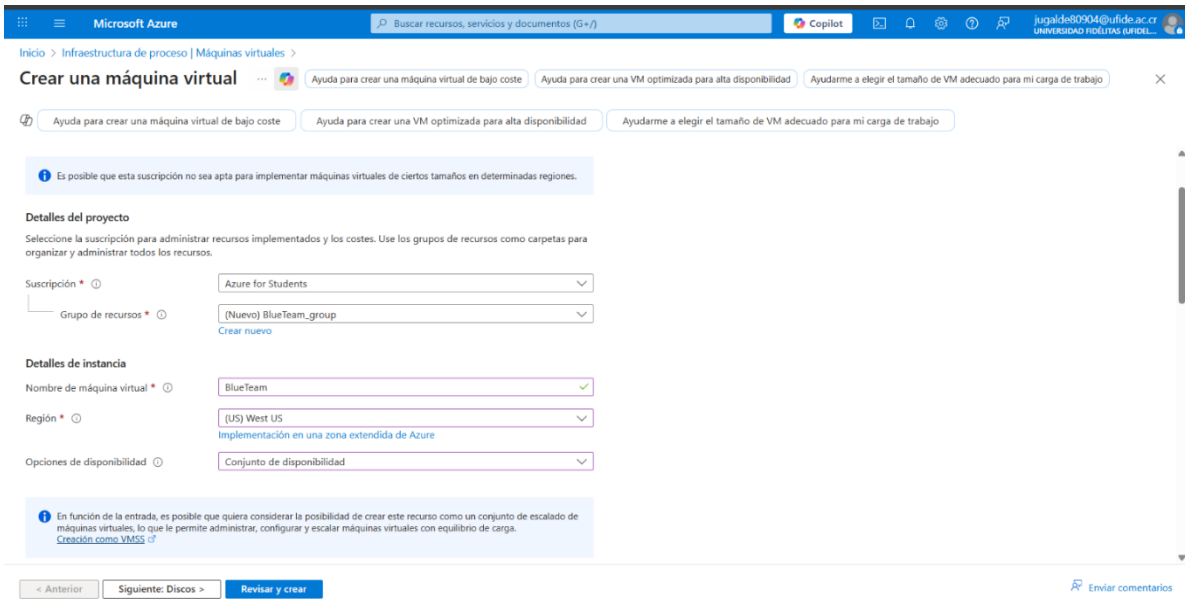
Profesor. Andrés Felipe Vargas Rivera

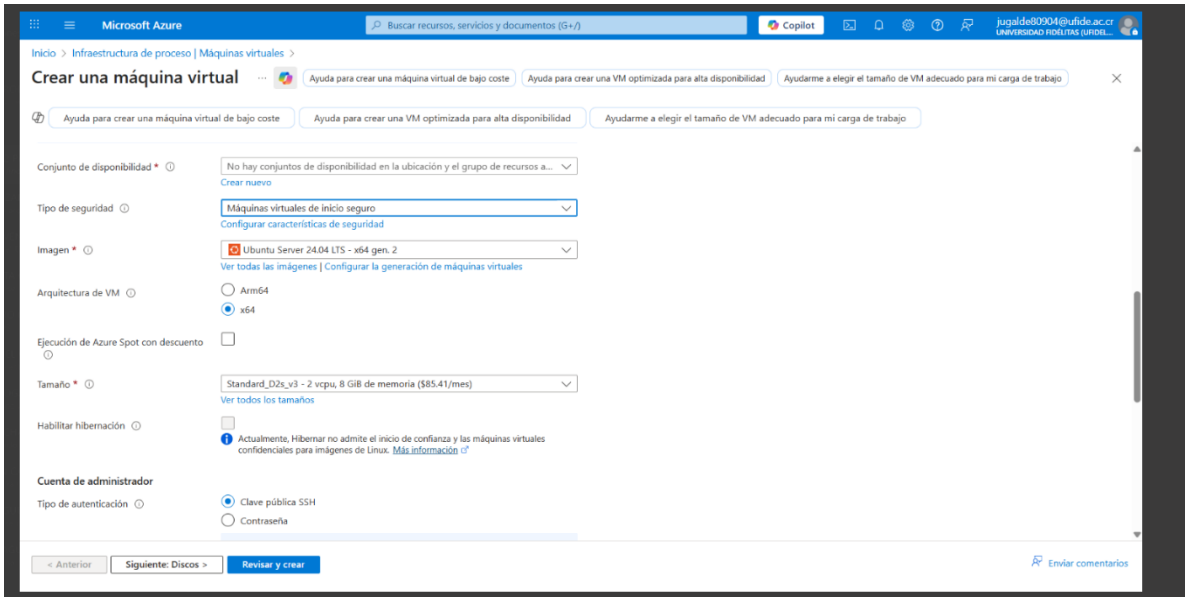
III Cuatrimestre 2025

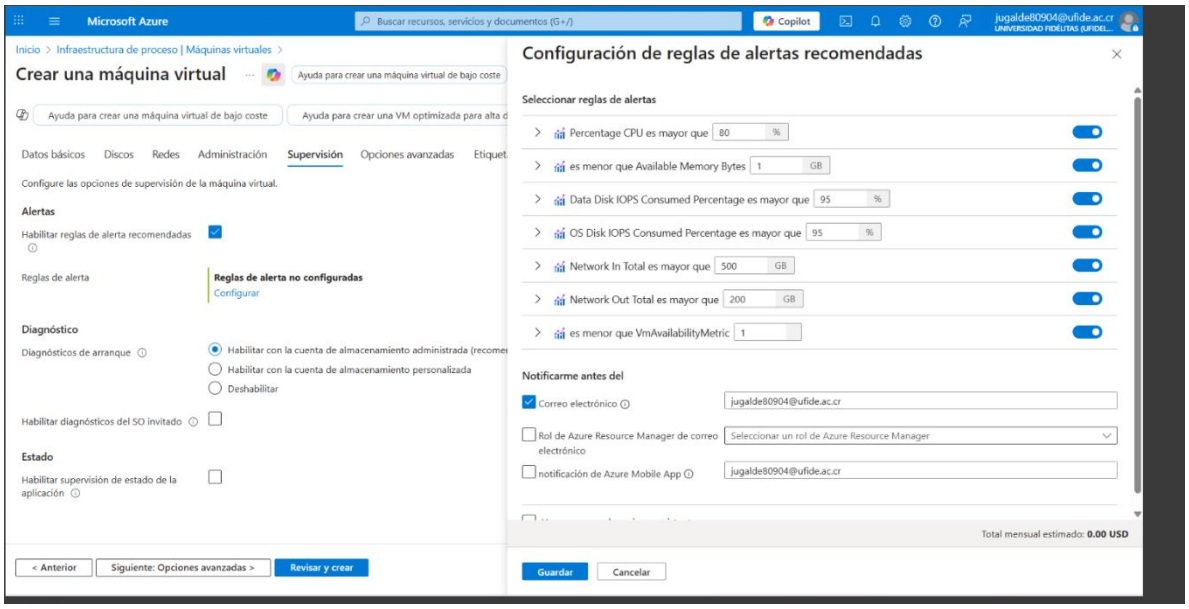
1.Roles del Equipo:

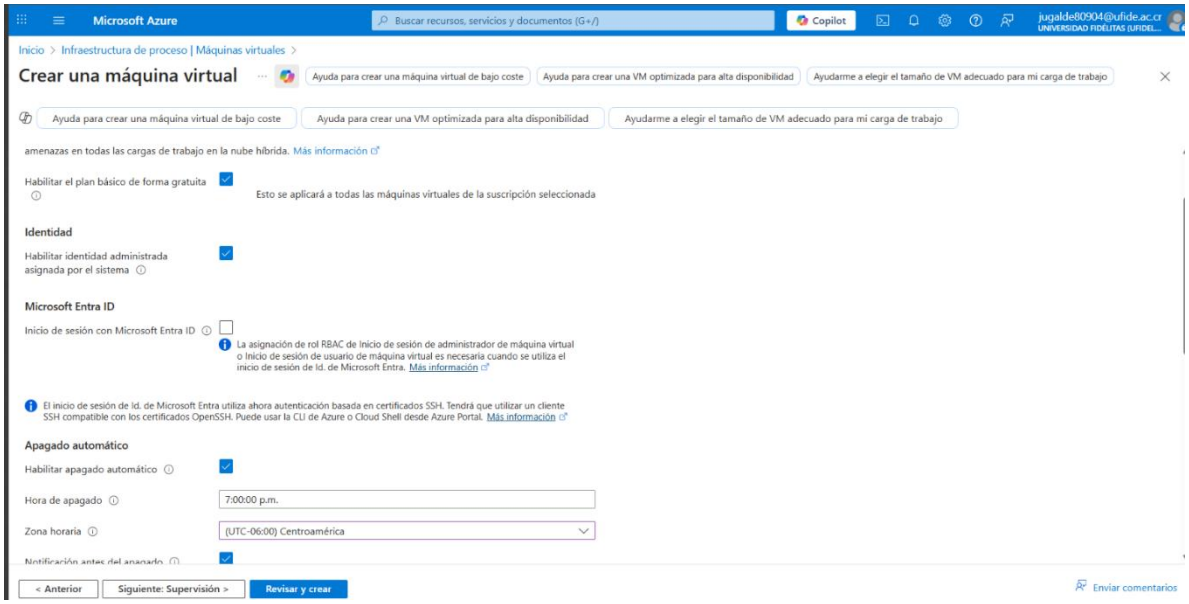
-Blue Team: Su rol es la de protector de ciberataques necesita conocer las formas y métodos de ataque para poder defenderse de los mismos. También hay medidas de que reducen la probabilidad de de ataques.

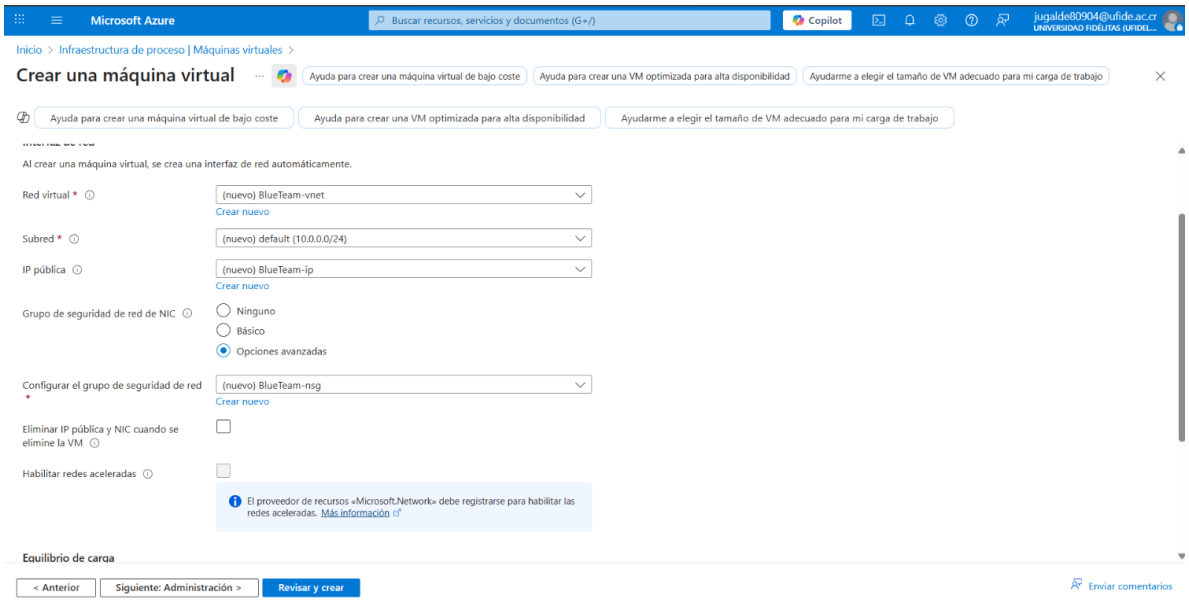
Crear y configurar la VM en Azure

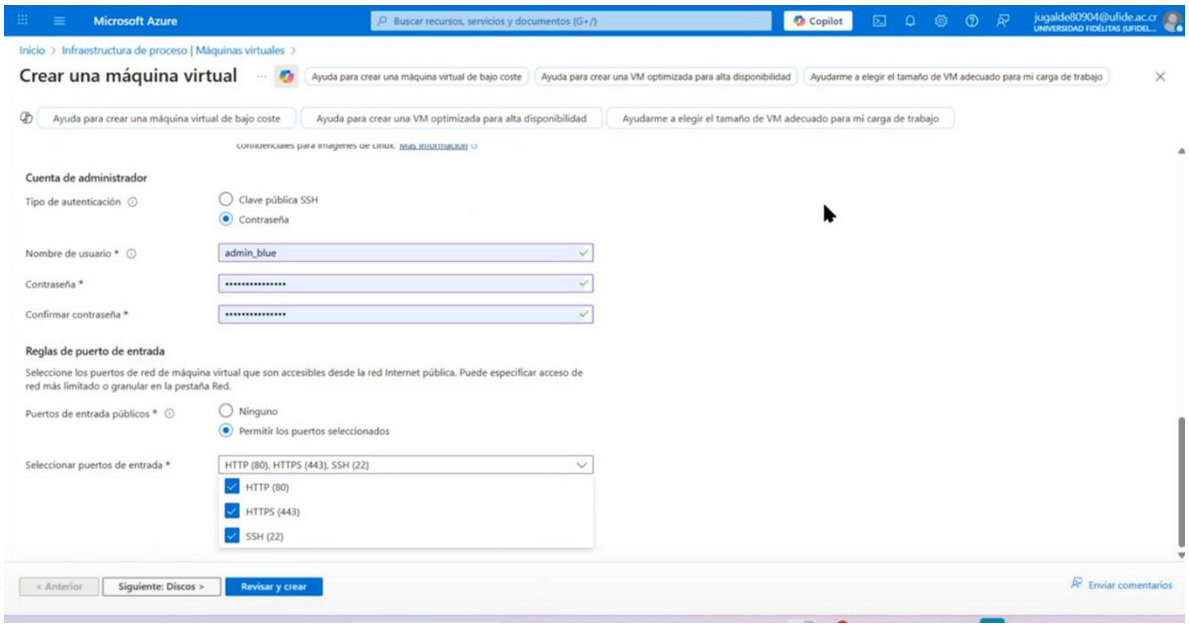


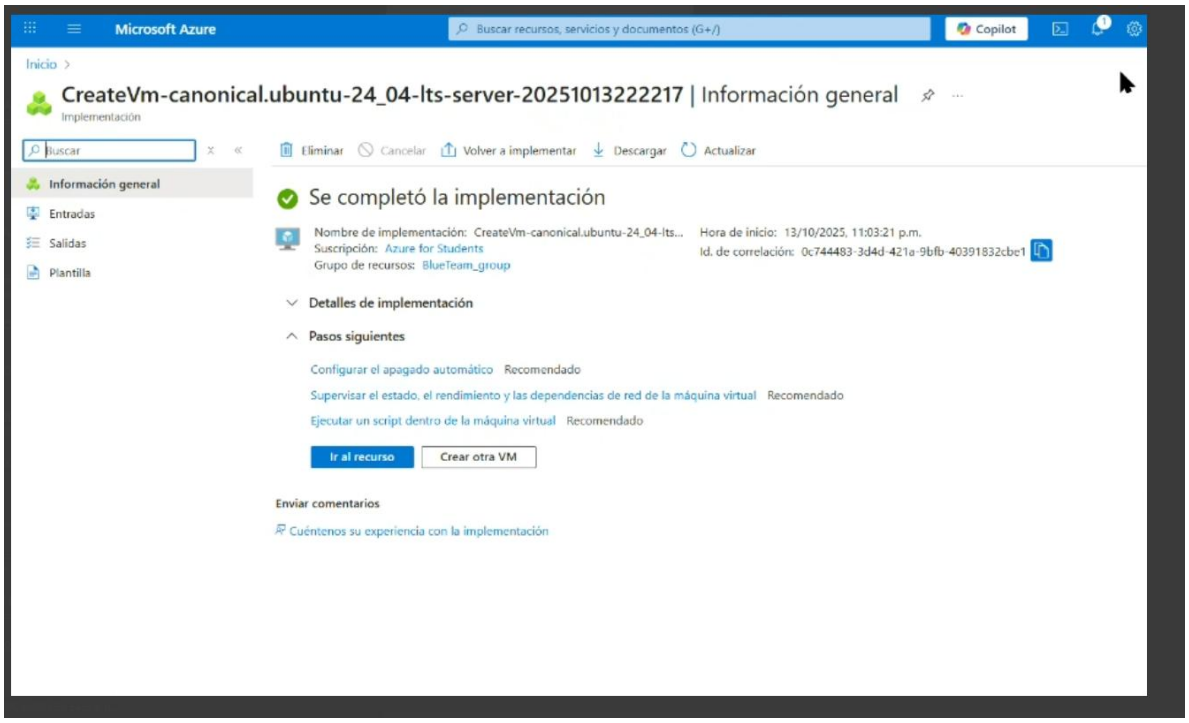



Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Copilot
jugalde80904@ufide.ac.cr
UNIVERSIDAD FIDÉLITAS (UFIDEL...
Inicio > Infraestructura de proceso | Máquinas virtuales >
Crear una máquina virtual
Ayuda para crear una máquina virtual de bajo coste
Ayuda para crear una VM optimizada para alta d
Datos básicos
Discos
Redes
Administración
Supervisión
Opciones avanzadas
Etiquet
Configure las opciones de supervisión de la máquina virtual.
Alertas
Habilitar reglas de alerta recomendadas
Reglas de alerta
Reglas de alerta no configuradas
Configurar
Diagnóstico
Diagnósticos de arranque
Habilitar con la cuenta de almacenamiento administrada (recome
Habilitar con la cuenta de almacenamiento personalizada
Deshabilitar
Habilitar diagnósticos del SO invitado
Estado
Habilitar supervisión de estado de la aplicación
< Anterior
Siguiente: Opciones avanzadas >
Revisar y crear
Configuración de reglas de alertas recomendadas
Seleccionar reglas de alertas
Percentage CPU es mayor que 80 %
es menor que Available Memory Bytes 1 GB
Data Disk IOPS Consumed Percentage es mayor que 95 %
OS Disk IOPS Consumed Percentage es mayor que 95 %
Network In Total es mayor que 500 GB
Network Out Total es mayor que 200 GB
es menor que VmAvailabilityMetric 1
Notificarme antes del
Correo electrónico
jugalde80904@ufide.ac.cr
Rol de Azure Resource Manager de correo electrónico
Seleccionar un rol de Azure Resource Manager
notificación de Azure Mobile App
jugalde80904@ufide.ac.cr
Total mensual estimado: 0.00 USD
Guardar
Cancelar


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Copilot
jugalde80904@ufide.ac.cr
UNIVERSIDAD FIDÉLITAS (UFIDEL...
Inicio > Infraestructura de proceso | Máquinas virtuales >
Crear una máquina virtual
Ayuda para crear una máquina virtual de bajo coste
Ayuda para crear una VM optimizada para alta disponibilidad
Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo
amenazas en todas las cargas de trabajo en la nube híbrida. Más información
Habilitar el plan básico de forma gratuita
Esto se aplicará a todas las máquinas virtuales de la suscripción seleccionada
Identidad
Habilitar identidad administrada asignada por el sistema
Microsoft Entra ID
Inicio de sesión con Microsoft Entra ID
La asignación de rol RBAC de Inicio de sesión de administrador de máquina virtual o Inicio de sesión de usuario de máquina virtual es necesaria cuando se utiliza el inicio de sesión de Id. de Microsoft Entra. Más información
El inicio de sesión de Id. de Microsoft Entra utiliza ahora autenticación basada en certificados SSH. Tendrá que utilizar un cliente SSH compatible con los certificados OpenSSH. Puede usar la CLI de Azure o Cloud Shell desde Azure Portal. Más información
Apagado automático
Habilitar apagado automático
Hora de apagado
7:00:00 p.m.
Zona horaria
(UTC-06:00) Centroamérica
Notificación antes del apagado
< Anterior
Siguiente: Supervisión >
Revisar y crear
Enviar comentarios


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Copilot
jugalde80904@ufide.ac.cr
UNIVERSIDAD FIDÉLITAS (UFIDEL...
Inicio > Infraestructura de proceso | Máquinas virtuales >
Crear una máquina virtual
Ayuda para crear una máquina virtual de bajo coste
Ayuda para crear una VM optimizada para alta disponibilidad
Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo
Al crear una máquina virtual, se crea una interfaz de red automáticamente.
Red virtual *
(nuevo) BlueTeam-vnet
Crear nuevo
Subred *
(nuevo) default (10.0.0.0/24)
IP pública
(nuevo) BlueTeam-ip
Crear nuevo
Grupo de seguridad de red de NIC
Ninguno
Básico
Opciones avanzadas
Configurar el grupo de seguridad de red *
(nuevo) BlueTeam-nsg
Crear nuevo
Eliminar IP pública y NIC cuando se elimine la VM
Habilitar redes aceleradas
El proveedor de recursos «Microsoft.Network» debe registrarse para habilitar las redes aceleradas. Más información
Equilibrio de carga
< Anterior
Siguiente: Administración >
Revisar y crear
Enviar comentarios


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Copilot
jugalde80904@ufide.ac.cr
UNIVERSIDAD FIDÉLITAS (UFIDEL...
Inicio > Infraestructura de proceso | Máquinas virtuales >
Crear una máquina virtual
Ayuda para crear una máquina virtual de bajo coste
Ayuda para crear una VM optimizada para alta disponibilidad
Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo
Cuenta de administrador
Tipo de autenticación
Clave pública SSH
Contraseña
Nombre de usuario *
admin_blue
Contraseña *
Confirmar contraseña *
Reglas de puerto de entrada
Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.
Puertos de entrada públicos *
Ninguno
Permitir los puertos seleccionados
Seleccionar puertos de entrada *
HTTP (80), HTTPS (443), SSH (22)
HTTP (80)
HTTPS (443)
SSH (22)
< Anterior
Siguiente: Discos >
Revisar y crear
Enviar comentarios



Pasos a seguir:

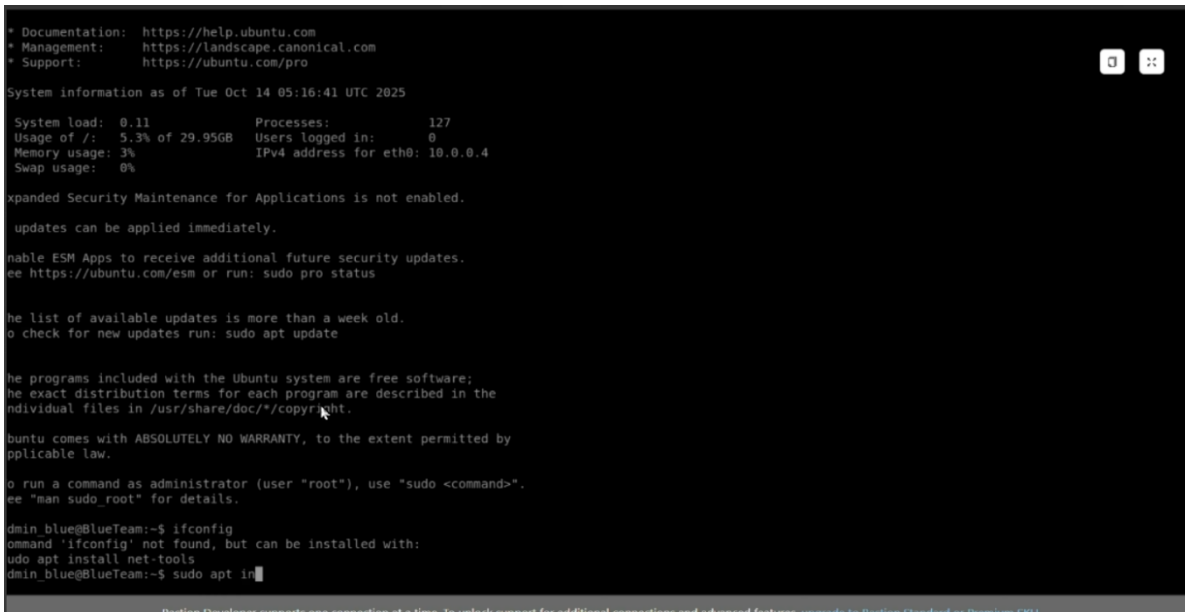
Desde el navegador con Azure Bastion (sin abrir puertos)

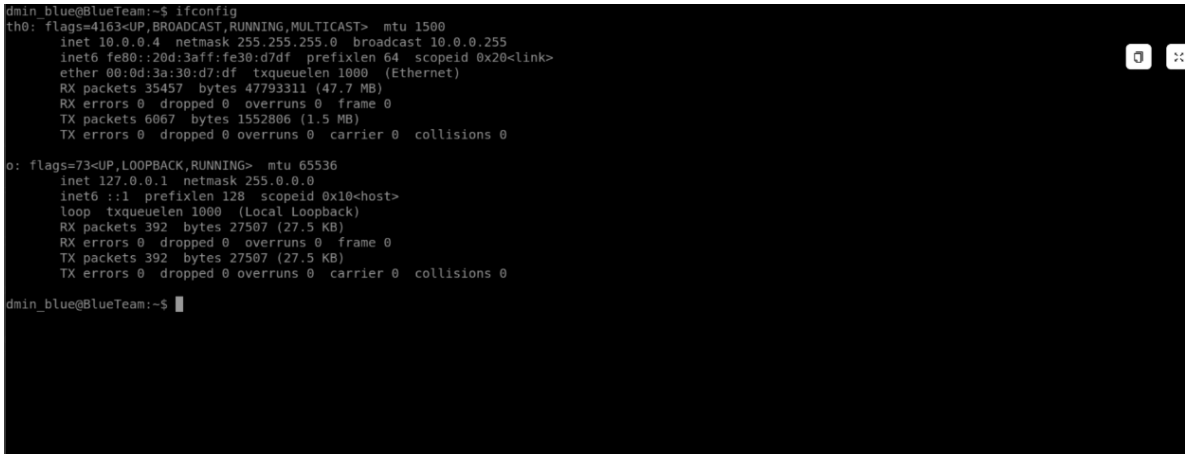
En el portal de la VM → botón Conectar → pestaña Bastion.

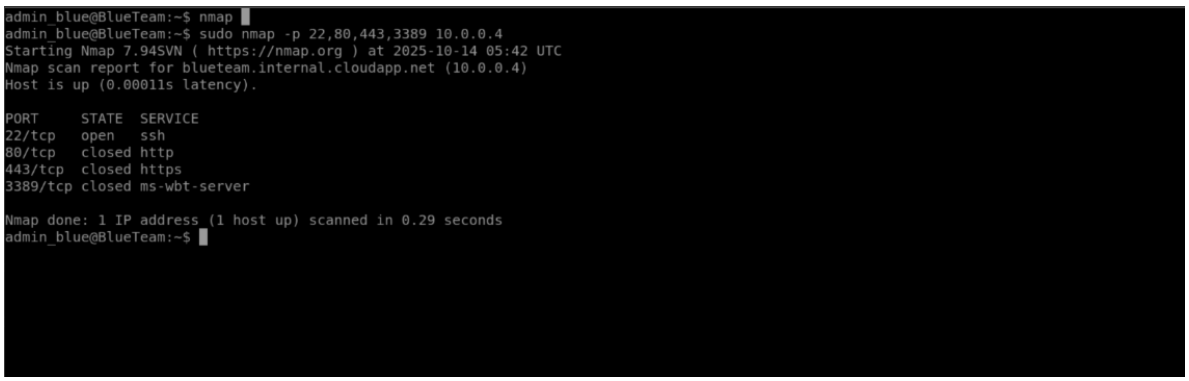
Si no está creado, haz Crear Bastion (sigue el asistente).

Rellena usuario y contraseña/clave → Conectar.

Resultado: consola SSH en el navegador.

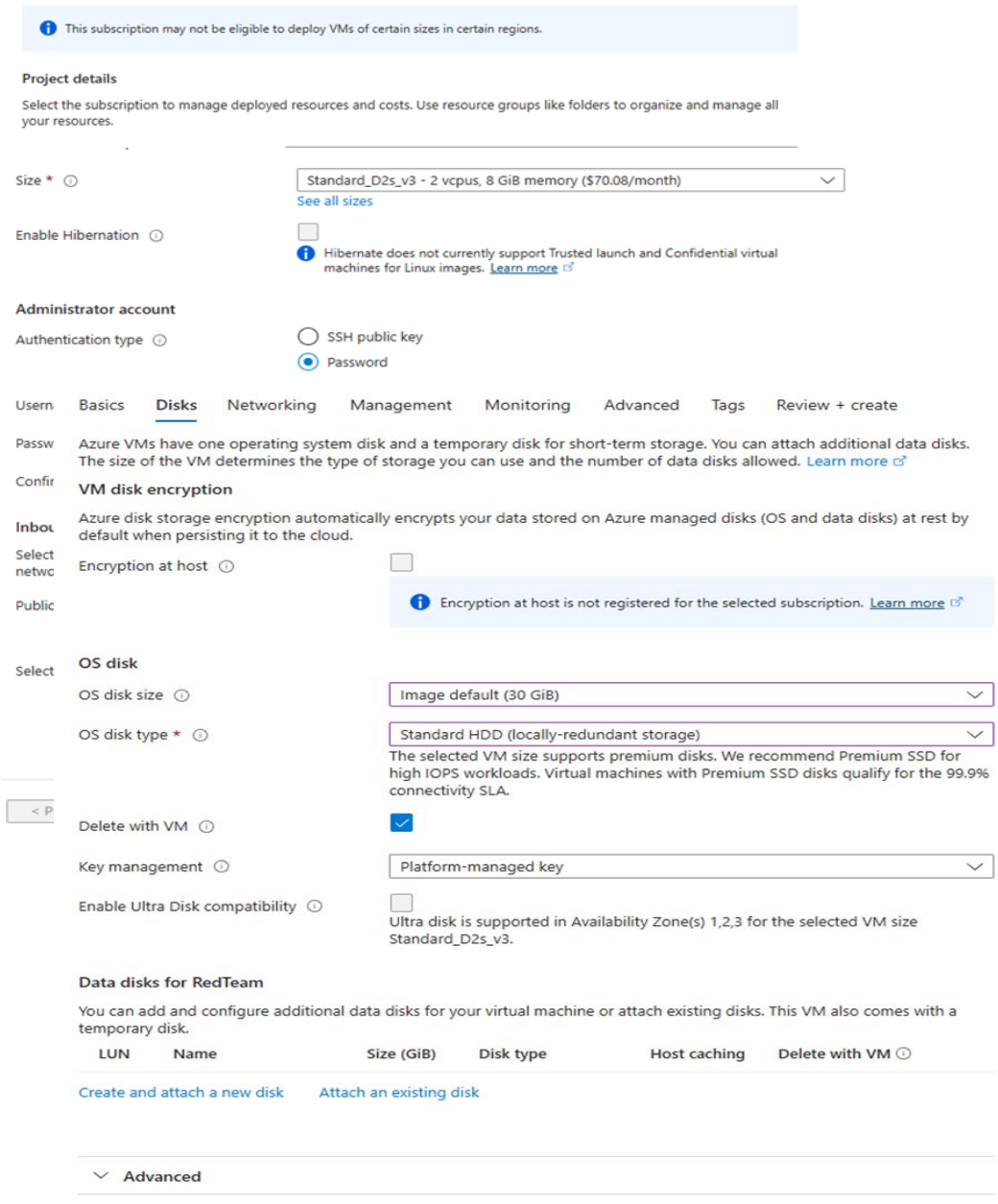

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Tue Oct 14 05:16:41 UTC 2025
System load: 0.11   Processes: 127
Usage of /:   5.3% of 29.95GB   Users logged in: 0
Memory usage: 3%   IPv4 address for eth0: 10.0.0.4
Swap usage: 0%
xpanded Security Maintenance for Applications is not enabled.
updates can be applied immediately.
nable ESM Apps to receive additional future security updates.
ee https://ubuntu.com/esm or run: sudo pro status
he list of available updates is more than a week old.
o check for new updates run: sudo apt update
he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.
buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.
o run a command as administrator (user "root"), use "sudo <command>".
ee "man sudo_root" for details.
dmin_blue@BlueTeam:~$ ifconfig
ommand 'ifconfig' not found, but can be installed with:
udo apt install net-tools
dmin_blue@BlueTeam:~$ sudo apt in


dmin_blue@BlueTeam:~$ ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.0.4 netmask 255.255.255.0 broadcast 10.0.0.255
inet6 fe80::20d:3aff:fe30:d7df prefixlen 64 scopeid 0x20<link>
ether 00:0d:3a:30:d7:df txqueuelen 1000 (Ethernet)
RX packets 35457 bytes 47793311 (47.7 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 6067 bytes 1552806 (1.5 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
o: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 392 bytes 27507 (27.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 392 bytes 27507 (27.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
dmin_blue@BlueTeam:~$


admin_blue@BlueTeam:~$ nmap
admin_blue@BlueTeam:~$ sudo nmap -p 22,80,443,3389 10.0.0.4
Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-14 05:42 UTC
Nmap scan report for blueteam.internal.cloudapp.net (10.0.0.4)
Host is up (0.00011s latency).
PORT   STATE SERVICE
22/tcp   open   ssh
80/tcp   closed http
443/tcp closed https
3389/tcp closed ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
admin_blue@BlueTeam:~$

-Red Team: Su rol es el de agresor virtual identifica y utiliza las vulnerabilidades del sistema o de los usuarios del sistema. Para modificar leer o ver datos confidenciales.

Creación y Configuración de la VM en Azure



Pasos a seguir:

Desde el navegador con Azure Bastion (sin abrir puertos)

En el portal de la VM → botón Conectar → pestaña Bastion.

Si no está creado, haz Crear Bastion (sigue el asistente).

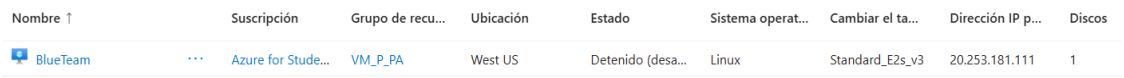
Rellena usuario y contraseña/clave → Conectar.

Resultado: consola SSH en el navegador.

2. IP de la Máquina Virtual Objetivo (BlueTeam):

Máquina Virtual Blue Team:

IP: 172.184.103.17



Nombre ↑	Suscripción	Grupo de recu...	Ubicación	Estado	Sistema operat...	Cambiar el ta...	Dirección IP p...	Discos
BlueTeam ···	Azure for Stude...	VM_P_PA	West US	Detenido (desa...	Linux	Standard_E2s_v3	20.253.181.111	1

3. Puertos Permitidos (NSG):

- SSH: 22

4. Buenas Prácticas de Seguridad:

-Mantener actualizado el sistema con `sudo apt update && sudo apt upgrade -y`.

- Apagar la VM cuando no esté en uso.

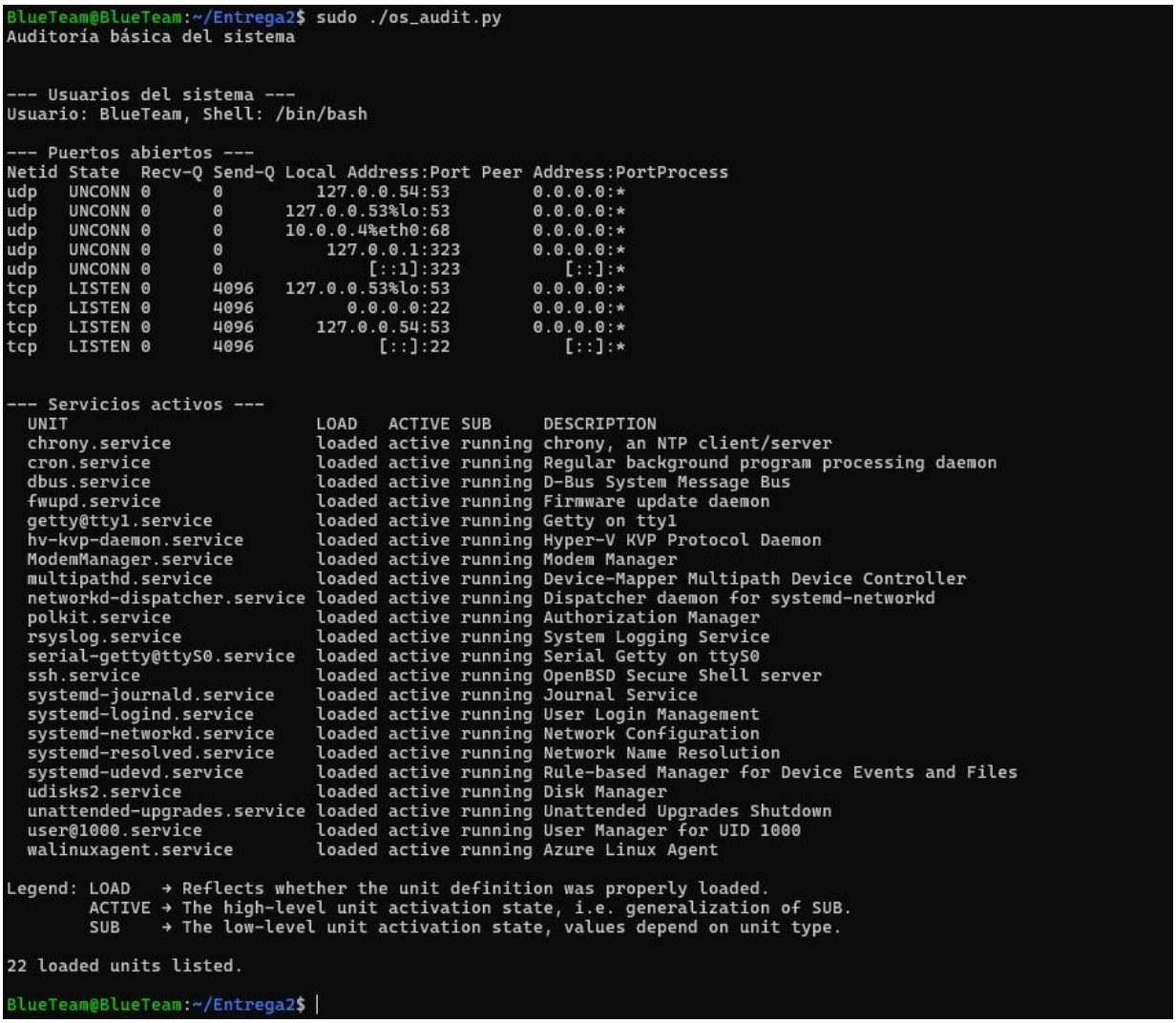
- Evitar exponer servicios innecesarios.

- Utilizar contraseñas y claves seguras.

- Supervisar accesos SSH desde direcciones IP conocidas

BlueTeam:

Usuarios, Puertos Abierto, Servicios Activos.



RedTeam:

No funciona Nmap en la maquina