



**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

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

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

Es posible que esta suscripción no sea apta para implementar máquinas virtuales de ciertos tamaños en determinadas regiones.

**Detalles del proyecto**

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción \*

Grupo de recursos \*  [Crear nuevo](#)

**Detalles de instancia**

Nombre de máquina virtual \*

Región \*  [Implementación en una zona extendida de Azure](#)

Opciones de disponibilidad

En función de la entrada, es posible que quiera considerar la posibilidad de crear este recurso como un conjunto de escalado de máquinas virtuales, lo que le permite administrar, configurar y escalar máquinas virtuales con equilibrio de carga. [Creación como VMSS](#)

< Anterior Siguiente: Discos > Revisar y crear

Enviar comentarios

Microsoft Azure

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

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

Conjunto de disponibilidad \*  [Crear nuevo](#)

Tipo de seguridad  [Configurar características de seguridad](#)

Imagen \*  [Ver todas las imágenes](#) | [Configurar la generación de máquinas virtuales](#)

Arquitectura de VM ☐ ☒

Ejecución de Azure Spot con descuento ☐

Tamaño \*  [Ver todos los tamaños](#)

Habilitar hibernación ☐ [Actualmente, Hibernar no admite el inicio de confianza y las máquinas virtuales confidenciales para imágenes de Linux. Más información](#)

**Cuenta de administrador**

Tipo de autenticación ☒ ☐

< Anterior Siguiente: Discos > Revisar y crear

Enviar comentarios

Microsoft Azure

Buscar recursos, servicios y documentos (G+)

Copilot

jugalde80904@ufide.ac.cr  
UNIVERSIDAD FIDELITAS (UFIDEL...)

Inicio > Infraestructura de proceso | Máquinas virtuales >

Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste

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

Etiquetas

Configure las opciones de supervisión de la máquina virtual.

Alertas

Habilitar reglas de alerta recomendadas

Reglas de alerta

Reglas de alerta no configuradas

Diagnóstico

Diagnósticos de arranque

Habilitar con la cuenta de almacenamiento administrada (recomendado)

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

Notifícame 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 FIDELITAS (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

Ayúdame a elegir el tamaño de VM adecuado para mi carga de trabajo

Ayuda para crear una máquina virtual de bajo coste

Ayuda para crear una VM optimizada para alta disponibilidad

Ayúdame 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 FIDELITAS (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

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 \*

Subred \*

IP pública

Grupo de seguridad de red de NIC

Configurar el grupo de seguridad de red \*

Eliminar IP pública y NIC cuando se elimine la VM

Habilitar redes aceleradas

(nuevo) BlueTeam-vnet  
[Crear nuevo](#)

(nuevo) default (10.0.0.0/24)  
[Crear nuevo](#)

(nuevo) BlueTeam-ip  
[Crear nuevo](#)

☐ Ninguno  
☐ Básico  
☒ Opciones avanzadas

(nuevo) BlueTeam-nsg  
[Crear nuevo](#)

☐

☐

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 FIDELITAS (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

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

Configuraciones para el agente de Linux. [Ver configuración](#)

Cuenta de administrador

Tipo de autenticación

Nombre de usuario \*

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 \*

Seleccionar puertos de entrada \*

☐ Clave pública SSH  
☒ Contraseña

admin\_blue

\*\*\*\*\*

\*\*\*\*\*

☐ Ninguno  
☒ Permitir los puertos seleccionados

HTTP (80), HTTPS (443), SSH (22)

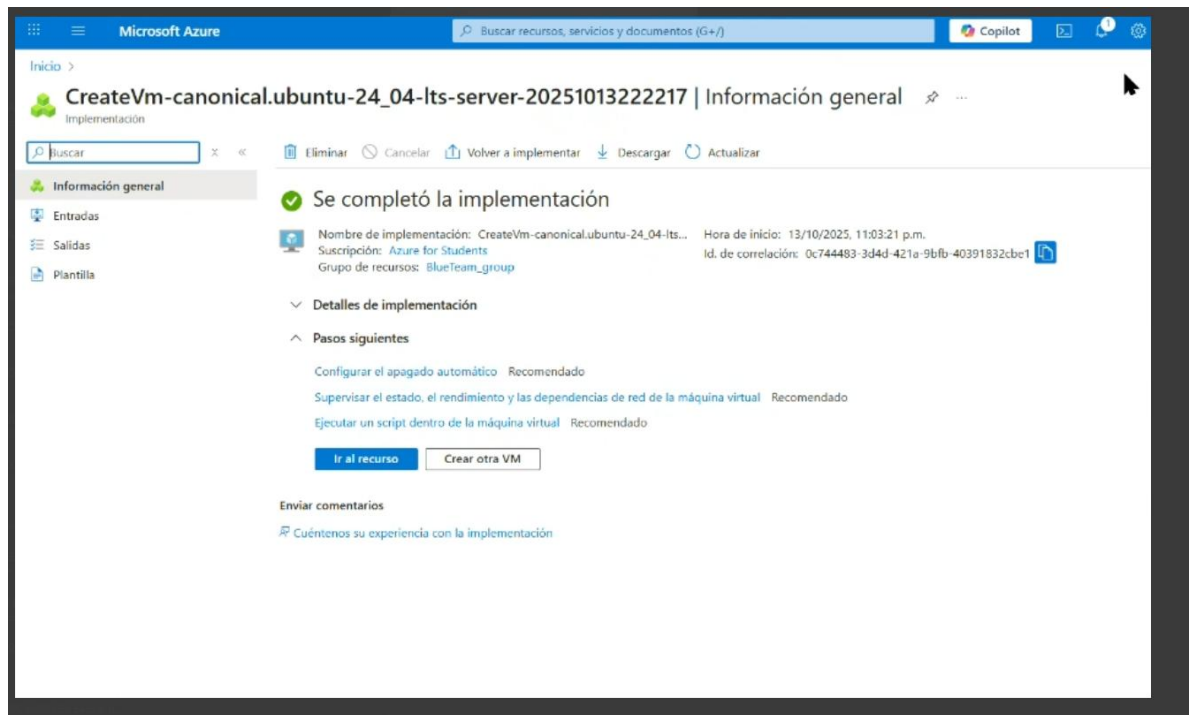
☒ HTTP (80)  
☒ HTTPS (443)  
☒ SSH (22)

< 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%
```

Expanded Security Maintenance for Applications is not enabled.

Updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.  
See <https://ubuntu.com/esm> or run: `sudo pro status`

The list of available updates is more than a week old.  
To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in `/usr/share/doc/*/*copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "`sudo <command>`".  
See "`man sudo_root`" for details.

```
dmin_blue@BlueTeam:~$ ifconfig
command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools
dmin_blue@BlueTeam:~$ sudo apt in
```

```
dmin_blue@BlueTeam:~$ ifconfig
eth0: 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

lo: 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:~\$

## Creación y Configuración de la VM en Azure

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Size \* ⓘ

Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$70.08/month) ⌵  
[See all sizes](#)

Enable Hibernation ⓘ

☐  
ⓘ Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#) ⓘ

Administrator account

Authentication type ⓘ

☐ SSH public key  
☒ Password

User Basics Disks Networking Management Monitoring Advanced Tags Review + create

Passw Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#) ⓘ

Confir VM disk encryption

Inbov Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.  
Select netwo Encryption at host ⓘ  
Public  
ⓘ Encryption at host is not registered for the selected subscription. [Learn more](#) ⓘ

Select OS disk

OS disk size ⓘ Image default (30 GiB) ⌵

OS disk type \* ⓘ Standard HDD (locally-redundant storage) ⌵  
The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

< P Delete with VM ⓘ ☒

Key management ⓘ Platform-managed key ⌵

Enable Ultra Disk compatibility ⓘ ☐  
Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_D2s\_v3.

Data disks for RedTeam

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ
Create and attach a new disk Attach an existing disk					

⌵ Advanced

Basics **Disks** Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

#### Basics

Subscription	Azure for Students
Resource group	(new) RedTeam_group
Virtual machine name	RedTeam
Region	West US 3

#### Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Backup	Disabled
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	Image Default

#### Monitoring

Alerts	Off
Boot diagnostics	On
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

#### Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

< Previous

Next >

Create

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.

```
BlueTeam@BlueTeam:~/Entrega2$ sudo ./os_audit.py
Auditoría básica del sistema

--- Usuarios del sistema ---
Usuario: BlueTeam, Shell: /bin/bash

--- Puertos abiertos ---
Netid State Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp UNCONN 0 0 127.0.0.54:53 0.0.0.0:*
udp UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:*
udp UNCONN 0 0 10.0.0.4%eth0:68 0.0.0.0:*
udp UNCONN 0 0 127.0.0.1:323 0.0.0.0:*
udp UNCONN 0 0 [::1]:323 [::]:*
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
tcp LISTEN 0 4096 0.0.0.0:22 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.54:53 0.0.0.0:*
tcp LISTEN 0 4096 [::]:22 [::]:*

--- Servicios activos ---
UNIT LOAD ACTIVE SUB DESCRIPTION
chrony.service loaded active running chrony, an NTP client/server
cron.service loaded active running Regular background program processing daemon
dbus.service loaded active running D-Bus System Message Bus
fwupd.service loaded active running Firmware update daemon
getty@tty1.service loaded active running Getty on tty1
hv-kvp-daemon.service loaded active running Hyper-V KVP Protocol Daemon
ModemManager.service loaded active running Modem Manager
multipathd.service loaded active running Device-Mapper Multipath Device Controller
networkd-dispatcher.service loaded active running Dispatcher daemon for systemd-networkd
polkit.service loaded active running Authorization Manager
rsyslog.service loaded active running System Logging Service
serial-getty@ttyS0.service loaded active running Serial Getty on ttyS0
ssh.service loaded active running OpenBSD Secure Shell server
systemd-journald.service loaded active running Journal Service
systemd-logind.service loaded active running User Login Management
systemd-networkd.service loaded active running Network Configuration
systemd-resolved.service loaded active running Network Name Resolution
systemd-udev.service loaded active running Rule-based Manager for Device Events and Files
udisks2.service loaded active running Disk Manager
unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
user@1000.service loaded active running User Manager for UID 1000
walinuxagent.service loaded active running Azure Linux Agent

Legend: LOAD → Reflects whether the unit definition was properly loaded.
ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
SUB → The low-level unit activation state, values depend on unit type.

22 loaded units listed.
BlueTeam@BlueTeam:~/Entrega2$ |
```

RedTeam:

No funciona Nmap en la maquina

```
RedTeam@RedTeam:~/Entrega2$ sudo ./scanner.py
Traceback (most recent call last):
  File "/home/RedTeam/Entrega2/./scanner.py", line 2, in <module>
    import nmap
ModuleNotFoundError: No module named 'nmap'
RedTeam@RedTeam:~/Entrega2$ |
```