



Architecture & Deployment

2025-2026 v0.1.0 on branch main Rev: 03b1cdace14bb0b0720e24be862097b3792214ea

Run your own virtual server on Microsoft Azure

This guide describes how to run a virtual server appropriate for the Media Engineering Architecture & Deployment course on the [Microsoft Azure](#) cloud platform.

Table of contents

- 📖 [Legend](#)
- ! [Apply to Azure for Students](#)
- ! [Get your public SSH key](#)
- ! [Launch a virtual server](#)
 - ! [Configure basic settings](#)
 - ! [Configure your administrator account](#)
 - ! [Make sure the SSH port is open](#)
 - ! [Skip the disk settings](#)
 - ! [Configure open ports](#)
 - ! [Skip advanced settings](#)
 - ! [Review your monthly cost](#)
 - ! [Create your server](#)
- ? [\(Optionally\) get your machine's public SSH key](#)
- ! [Configure your virtual server](#)
 - ! [Connect to your new virtual machine over SSH](#)
 - ! [Give the teacher access to your virtual machine](#)
 - ! [Change the hostname of your virtual machine](#)
 - ! [Reboot the server](#)
 - ! [Add swap space to your virtual server](#)
- ! [Register your Azure VM with us](#)
- 🏁 [What have I done?](#)
- ☀️ [Troubleshooting](#)
 - ☀️ [I forgot to open some \(or all\) of the ports in the firewall](#)

-  Azure complains that my RSA key is too short

Cloud server exercise

Parts of this exercise happen on the cloud server you should have created for this course. Log in and make sure you are connected to the internet to see your server's details.

Log in

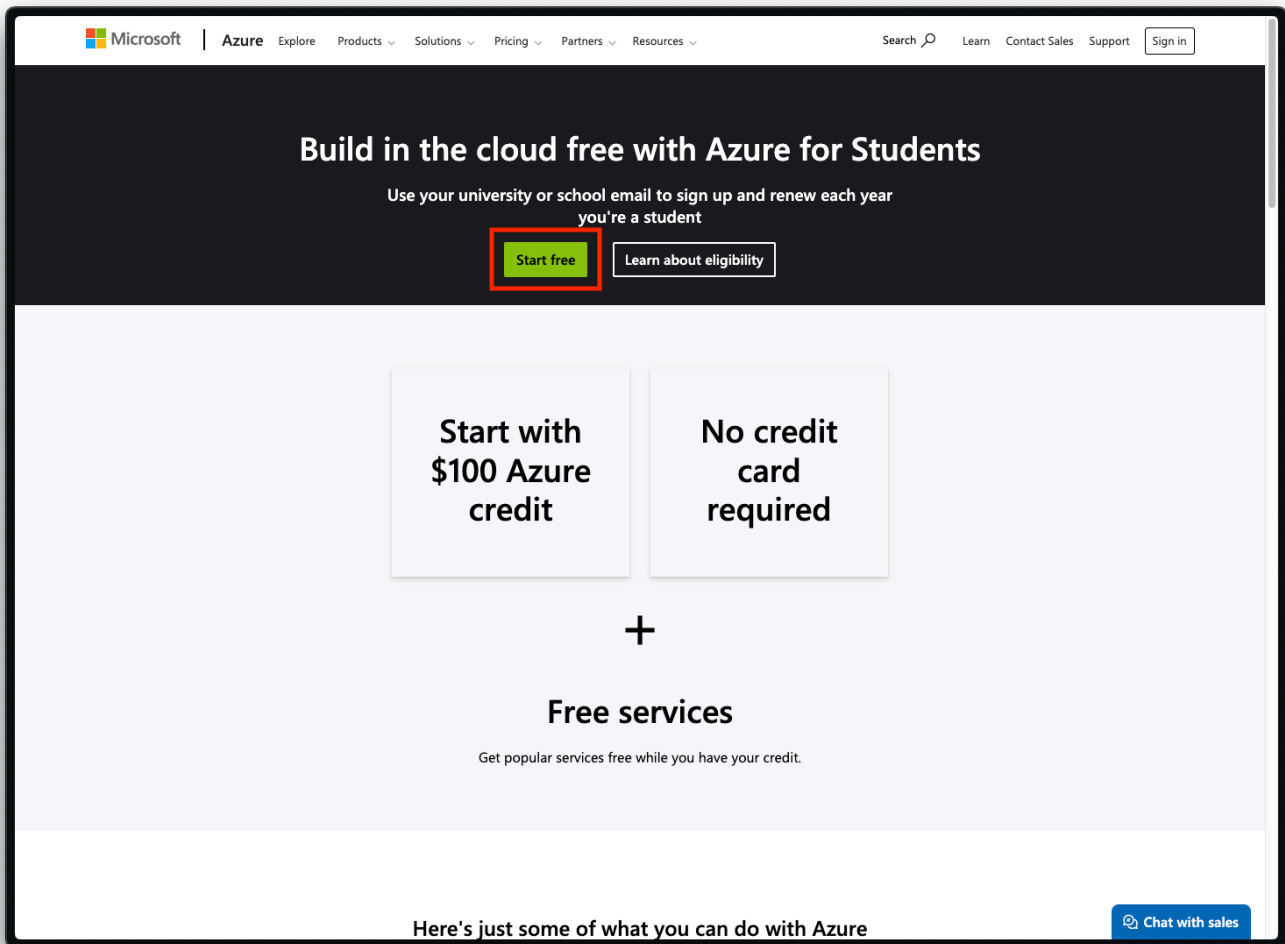
Legend

Parts of this exercise are annotated with the following icons:

- ! A task you **MUST** perform to complete the exercise
- ? An optional step that you may perform to make sure that everything is working correctly, or to set up additional tools that are not required but can help you
- 🏁 The end of the exercise
- 🏠 The architecture of the software you ran or deployed during this exercise.
- ☀️ Troubleshooting tips: how to fix common problems you might encounter

! Apply to Azure for Students

Apply to Azure for Students with your `@hes-so.ch` email address, which will provide you with free Azure resources as a student.



! Get your public SSH key

You can display your public SSH key in your terminal with the following command:

```
$> cat ~/.ssh/id_ed25519.pub
```

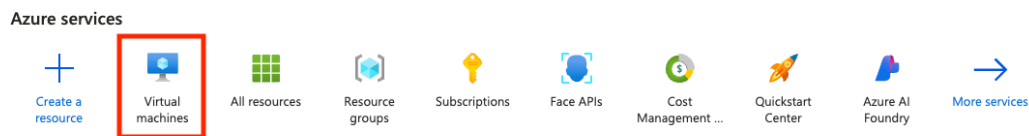
Tip

If you have an older SSH client, you may want to try displaying the contents of `~/.ssh/id_rsa.pub` instead.

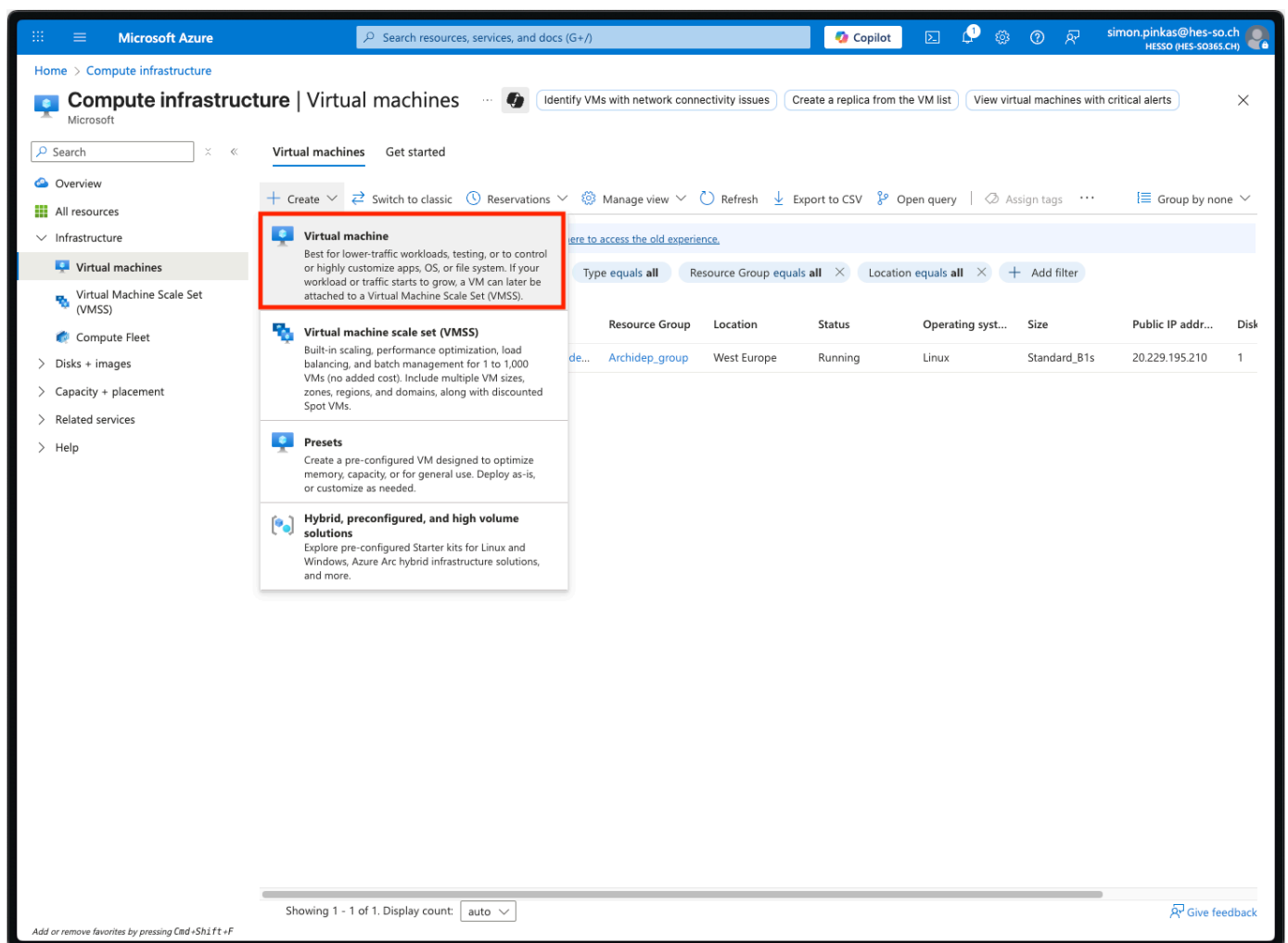
! Launch a virtual server

Once you have your Azure account, you can launch the virtual server you will be using for the rest of the course.

Access the Azure portal and go to the **Virtual machines** section:



Create a new virtual machine, i.e. a new virtual server in the Microsoft Azure infrastructure:



! Configure basic settings

In the **Basics** settings, configure the **virtual machine details** (the machine's name, region, image and size):

Create a virtual machine ...

- Help me create a low cost VM
- Help me create a VM optimized for high availability
- Help me choose the r

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ

HEIG-VD

Resource group * ⓘ

(New) ArchiDep_group

Create new

Instance details

Virtual machine name * ⓘ

ArchiDep

Region * ⓘ

(Europe) West Europe

Availability options ⓘ

Availability zone

Zone options ⓘ

☒ Self-selected zone
Choose up to 3 availability zones, one VM per zone

☐ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * ⓘ

Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ

Trusted launch virtual machines

[Configure security features](#)

Image * ⓘ

Ubuntu Server 24.04 LTS - x64 Gen2

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

☐ Arm64

☒ x64

Run with Azure Spot discount ⓘ

☐

Size * ⓘ

Standard_B1s - 1 vcpu, 1 GiB memory (\$8.76/month)

[See all sizes](#)

Enable Hibernation ⓘ

☐

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

⚠ **Make sure to select the **Ubuntu 24.04** image and the **B1s** size.** If you select a VM size that is too expensive, **YOU WILL RUN OUT OF FREE CREDITS BEFORE THE END OF THE COURSE** You will then have to pay 💰 for a new VM and will have to reinstall your VM from scratch (including all deployment exercises you may already have completed).

🔥 Troubleshooting

If the correct size is not selected, you can select it from the complete list of VM sizes. If you cannot select the **B1s** size, try selecting another availability zone (or another region that is not too expensive).

Select a VM size ...

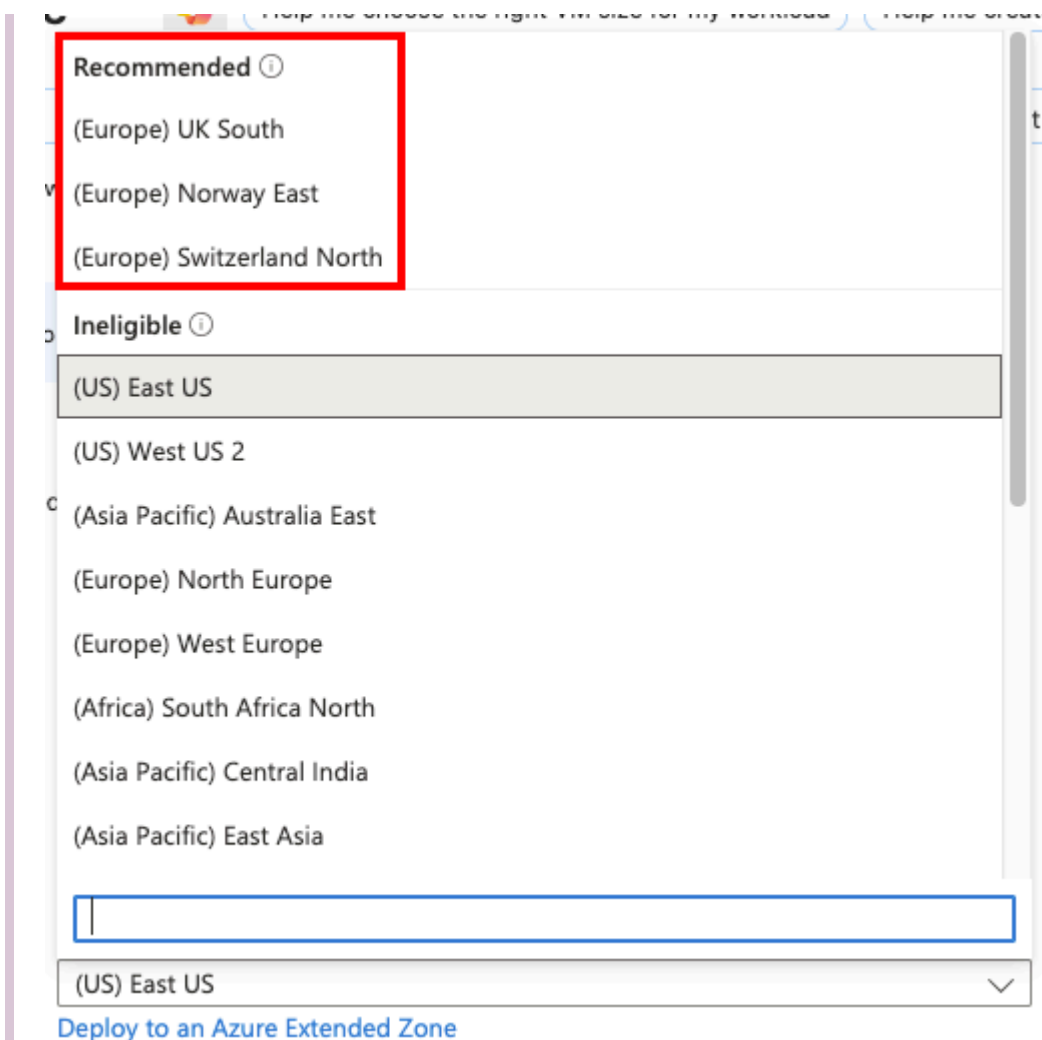
Search by VM size... vCPUs : All RAM (GiB) : All Display cost : Monthly Add filter

Showing 833 VM sizes. Subscription: HEIG-VD Region: West Europe Current size: Standard_B1s Image: Ubuntu Server 24.04 LTS Learn more about VM sizes Group by series

VM Size ↑↓	Type ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Local storage (GiB) ↑↓	Premium disk ↑↓	Cost/month ↑↓
> Most used by Azure users								
> D-Series v4								
The 4th generation D family sizes for your general purpose needs								
▼ B-Series								
Ideal for workloads that do not need continuous full CPU performance								
B2s	General purpose	2	4	4	1280	8 (SCSI)	Supported	\$35.04
B1s	General purpose	1	1	2	320	4 (SCSI)	Supported	\$8.76
B2ms	General purpose	2	8	4	1920	16 (SCSI)	Supported	\$70.08
B1ls	General purpose	1	0.5	2	320	4 (SCSI)	Supported	\$4.38
B4ms	General purpose	4	16	8	2880	32 (SCSI)	Supported	\$140.16
B1ms	General purpose	1	2	2	640	4 (SCSI)	Supported	\$17.52
B8ms	General purpose	8	32	16	4320	64 (SCSI)	Supported	\$280.32
> DC-Series								
Designed to protect the confidentiality and integrity of code and data for general-purpose workloads								
▼ F-Series								
The 4th generation F family sizes for your high memory needs								

💡 Tip

As a student, you are not allowed to run your virtual machine in any region. Choose one of the regions that are recommended for you (these may be different for each student):



The screenshot shows the Azure portal's region selection interface. It is divided into two main sections: 'Recommended' and 'Ineligible'. The 'Recommended' section is highlighted with a red box and contains three options: '(Europe) UK South', '(Europe) Norway East', and '(Europe) Switzerland North'. The 'Ineligible' section contains a list of regions that are not recommended, including '(US) East US', '(US) West US 2', '(Asia Pacific) Australia East', '(Europe) North Europe', '(Europe) West Europe', '(Africa) South Africa North', '(Asia Pacific) Central India', and '(Asia Pacific) East Asia'. Below the list is a search bar and a dropdown menu currently showing '(US) East US'. At the bottom, there is a link that says 'Deploy to an Azure Extended Zone'.

Recommended ⓘ

- (Europe) UK South
- (Europe) Norway East
- (Europe) Switzerland North

Ineligible ⓘ

- (US) East US
- (US) West US 2
- (Asia Pacific) Australia East
- (Europe) North Europe
- (Europe) West Europe
- (Africa) South Africa North
- (Asia Pacific) Central India
- (Asia Pacific) East Asia

Search

(US) East US

[Deploy to an Azure Extended Zone](#)

In general, choosing a region closer to where you are (or where your customers are) will reduce latency, and the North/West European regions are among the cheapest.

! Configure your administrator account

Under the **Administrator account** settings, configure your username.



Replace `jde` with the username you have selected for the course.

Administrator account

Authentication type ⓘ

☒ SSH public key

☐ Password

i Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ

jde

SSH public key source

Use existing public key

g Ed25519 and RSA SSH formats are supported for the selected VM image. Ed25519 offers better performance and security with a smaller key size, while RSA is still widely used particularly for legacy systems and applications.

SSH public key * ⓘ

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJNeZvBtr4u3/  
AmifDO90CJlKeB2xFMxI jde
```

i [Learn more about creating and using SSH keys in Azure](#)

Select **SSH public key** authentication, set the source to **Use existing public key**, and paste your public SSH key (the one you copied earlier) in the text area.

Warning

Your Unix username MUST NOT contain spaces, accented characters (e.g. é), hyphens (-) or dots (.). If you use the same name later in the course as a subdomain, it **MUST NOT** contain any underscores (_). We suggest you choose a name that starts with a letter (a-z) and contains only alphanumeric characters (a-z and 0-9).

Tip

Choose a username that is simple to type because you will need to type it often. If necessary, you can change it later.

Make sure the SSH port is open

Under inbound port rules, make sure the SSH (22) port is allowed:

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

- ☐ None
- ☒ Allow selected ports

Select inbound ports *

SSH (22)

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Next, go to the **Disks** settings (**DO NOT** create the machine just yet):

< Previous

Next : Disks >

! Skip the disk settings

Keep the default **Disks** settings and go to the **Networking** settings:

< Previous

Next : Networking >

! Configure open ports

In the **Networking** settings, select the **Advanced** security group option, and create a new security group:

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<div>(new) ArchiDep-vnet</div> <div>Create new</div>
Subnet *	<div>(new) default (10.0.0.0/24)</div>
Public IP	<div>(new) ArchiDep-ip</div> <div>Create new</div>
NIC network security group	<div> <input type="radio"/> None <input type="radio"/> Basic <input checked="" type="radio"/> Advanced </div>
Configure network security group *	<div></div> <div>Create new</div>
Delete public IP and NIC when VM is deleted	<input checked="" type="checkbox"/>
Enable accelerated networking	<input type="checkbox"/>

The selected VM size does not support accelerated networking.

Add two inbound rules, one for **HTTP** and one for **HTTPS**:

Home > Virtual machines > Create a virtual machine >

Create network security group

Name *

ArchiDep-nsg

Inbound rules

1000: default-allow-ssh

Any

SSH (TCP/22)

+ Add an inbound rule

Outbound rules

No results

+ Add an outbound rule

OK

Add inbound security rule

ArchiDep-nsg

Source

Any

Source port ranges *

*

Destination

Any

Service

HTTP

Destination port ranges

80

Protocol

☐ Any
 ☒ TCP
 ☐ UDP
 ☐ ICMP

Action

☒ Allow
 ☐ Deny

Priority *

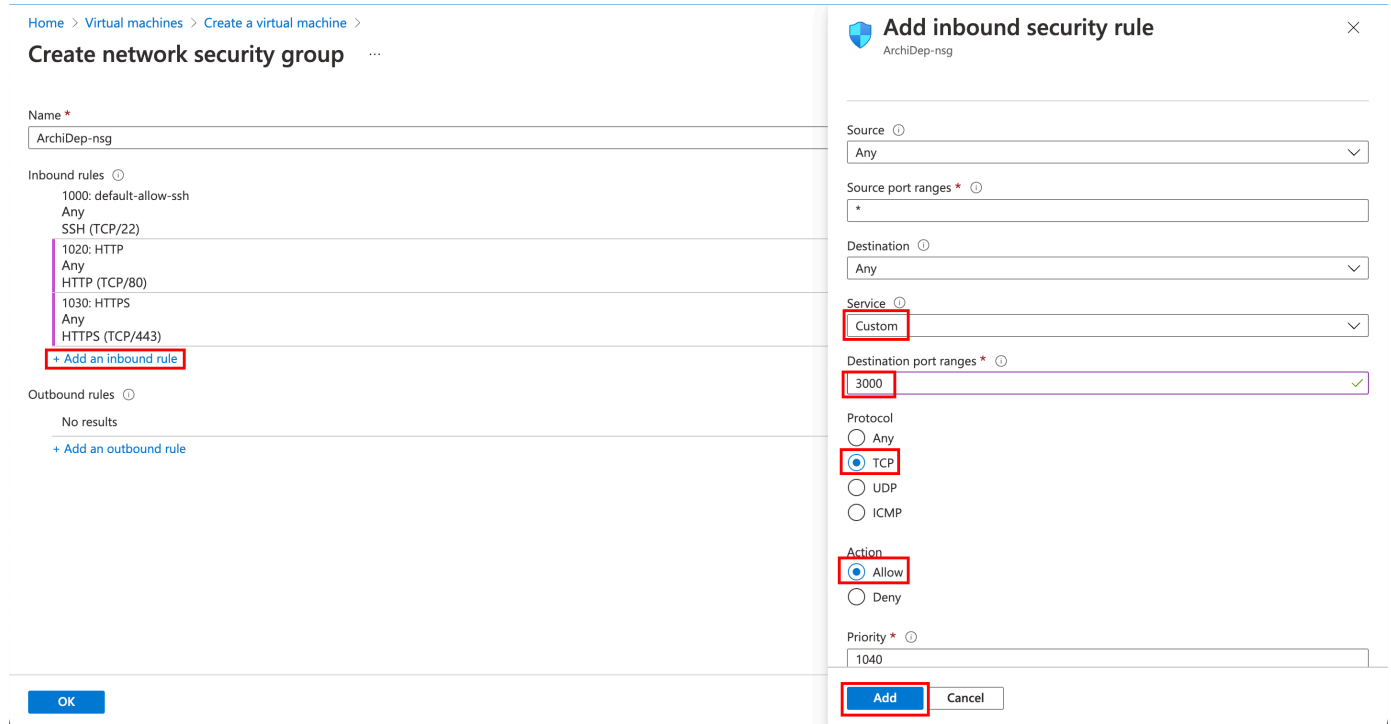
1020

Add Cancel

Tip

You will also have to name them. You can simply name them “HTTP” and “HTTPS”.

Add two other inbound rules, one for **port 3000** and one for **port 3001**:



The screenshot shows the Azure portal interface for creating a network security group. On the left, the 'Create network security group' page is visible, showing a list of inbound rules. The 'Add an inbound rule' button is highlighted with a red box. On the right, the 'Add inbound security rule' dialog is open, showing the configuration for a new rule. The 'Source' is set to 'Any', 'Source port ranges' is set to '*', 'Destination' is set to 'Any', 'Service' is set to 'Custom', 'Destination port ranges' is set to '3000', 'Protocol' is set to 'TCP', 'Action' is set to 'Allow', and 'Priority' is set to '1040'. The 'Add' button is highlighted with a red box.

Home > Virtual machines > Create a virtual machine > Create network security group ...

Name *
ArchiDep-nsg

Inbound rules ⓘ
1000: default-allow-ssh
Any
SSH (TCP/22)
1020: HTTP
Any
HTTP (TCP/80)
1030: HTTPS
Any
HTTPS (TCP/443)
+ Add an inbound rule

Outbound rules ⓘ
No results
+ Add an outbound rule

Add inbound security rule ArchiDep-nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
3000 ✓

Protocol
☒ Any
☒ TCP
☐ UDP
☐ ICMP

Action
☒ Allow
☐ Deny

Priority * ⓘ
1040

Add Cancel

Tip

You can simply name those rules “Port3000” and “Port3001”.

The final security group settings should look something like this:

Inbound rules ⓘ

1000: default-allow-ssh

Any

SSH (TCP/22)

1010: AllowAnyHTTPInbound

Any

HTTP (TCP/80)

1020: AllowAnyHTTPSInbound

Any

HTTPS (TCP/443)

1030: AllowAnyCustom3000Inbound

Any

Custom (TCP/3000)

1040: AllowAnyCustom3001Inbound

Any

Custom (TCP/3001)

[+ Add an inbound rule](#)



What you are doing here is configuring the Azure firewall to allow incoming traffic to your virtual server on specific ports. If you do not do this, it will not be reachable from outside the Azure network.

For example, for a web application running on your virtual server to be reachable, ports 80 (HTTP) and 443 (HTTPS) must accept incoming requests. Port 22 is for SSH connections. Ports 3000 and 3001 will be used in various exercises.

! Skip advanced settings

Keep the default **Management**, **Monitoring**, **Advanced** and **Tags** settings.

! Review your monthly cost

Review your estimated monthly cost:

Estimated monthly cost



\$17.34 / month

[View cost details](#)

You might not see the estimated monthly cost, but you should always see the hourly cost:

Price

1 X Standard B1s

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

0.0120 USD/hr

[Pricing for other VM sizes](#)



Your estimated monthly cost **MUST BE UNDER \$20/month OR UNDER \$0.025/hour**. If it is higher, you have probably selected the wrong region, or a VM size that is not the recommended one and that is too expensive for the credits you have at your disposal for this course.

! Create your server

Double-check that you are launching one virtual machine of size **B1s** (**1 X Standard B1s**).



Create your virtual machine!

☀ Troubleshooting

If Azure tells you that you cannot create a virtual machine in the region you have selected, go back to the [basic settings](#) and find a region that works. **Make sure to re-check your estimated monthly cost afterwards.**

Once your deployment is complete, go to the virtual machine source:

✓ Your deployment is complete



Deployment name: CreateVm-canonical.0001-com-ubuntu-server-f...
Subscription: [Azure subscription 1](#)
Resource group: [ArchiDep_group](#)

Start time: 10/15/2021, 12:45:01 PM
Correlation ID: 17f785a0-c447-4ca5-a847-203ab73d6110

▼ **Deployment details** ([Download](#))

^ **Next steps**

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#)

[Create another VM](#)

Find your machine's public IP address in the virtual machine's information:

The screenshot shows the Azure portal interface for a virtual machine named 'ArchiDep'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Security, Advisor recommendations, Extensions, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, and Locks. The main area displays the 'Essentials' section with a warning that the virtual machine agent status is not ready. Below this, the 'Properties' tab is active, showing details for the 'Virtual machine' such as Computer name (ArchiDep), Health state (-), Operating system (Linux), Publisher (canonical), Offer (0001-com-ubuntu-server-focal), Plan (20.04 LTS), VM generation (V2), Agent status (Not Ready), Agent version (Unknown), and Host group (None). The 'Networking' section shows the Public IP address as 20.71.227.143, Private IP address (IPv6) as -, Private IP address (IPv4) as 10.0.0.4, Virtual network/subnet as ArchiDep_group-vnet/default, and DNS name as Configure. The 'Size' section shows the Size as Standard B1s, vCPUs as 1, and RAM as 1 GiB.

? (Optionally) get your machine's public SSH key

When you connect to your virtual machine over SSH for the first time, you will get the usual warning that its authenticity cannot be verified:

```
The authenticity of host '20.71.227.143 (20.71.227.143)' can't be established.  
ECDSA key fingerprint is SHA256:0T0RCgUgzrPGeDHZV5fGAarkpGpc5Nbkhb7q2dbG00A.
```

Are you sure you want to continue connecting (yes/no/[fingerprint])?

To protect yourself from man-in-the-middle attacks, you can obtain the SSH host key fingerprints from your virtual machine before attempting to connect. That way, you will be able to see if the key fingerprint in the warning matches one of your virtual machine's keys.

To do this, you need to install the [Azure CLI](#). Once you have it installed and have logged in, you can run the following command (adapt the resource group and name options to your configuration if necessary):

```
$> az vm run-command invoke \
    --resource-group ArchiDep_group \
    --name ArchiDep \
    --command-id RunShellScript \
    --scripts "find /etc/ssh -name '*.pub' -exec ssh-keygen -l -f {} \;"
```

After a while, it should print the response:

```
{
  "value": [
    {
      "code": "ProvisioningState/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "Enable succeeded: \n[stdout]\n256 SHA256:IKNmtqj10KCP4gyErIaQkBI",
      "time": null
    }
  ]
}
```

Your machine's public key fingerprints are in the `message` property, separated by encoded new lines (`\n`).



You can skip this step if you consider the risk and impact of an attack low enough. Understand that if you simply answer “yes” when the SSH client warns you, you are exposing yourself to a potential man-in-the-middle attack. In all likelihood, no one is trying to hack your Azure virtual machine for this course, but the possibility exists.

Since you are using public key authentication and not password authentication, your credentials should not be compromised (you will not send a password and your private key will not leave your computer). However, anything you do on that server could potentially be read and modified by an attacker if he manages to intercept the initial connection.

! Configure your virtual server

You will now connect to your Azure virtual machine and configure some things for purposes of the course.

! Connect to your new virtual machine over SSH

Connect to your virtual machine using the `ssh <username>@<host>` command, replacing `<username>` with the username you chose for the course (the one you used for the machine’s administrator account), and `<host>` with the IP address you copied from the virtual machine’s information.

```
$> ssh jde@87.61.43.210
```



More information

You should be able to connect without a password. This works because you gave your public SSH key to Azure when creating your virtual server. It was automatically

put in your user's `~/.ssh/authorized_keys` file when the server was launched, which allows you to authenticate using your private SSH key.

! Give the teacher access to your virtual machine

Once you are connected, run the following command to give the teacher access to your virtual machine (**be sure to copy the whole line**):

```
$> echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB1TC4ygWjzpRemd0yrtqQYm0ARxMMks71fU"
```

More information

This adds the teacher's public SSH key to your user's `~/.ssh/authorized_keys`, allowing the teachers to also authenticate to your virtual server with their private SSH key to help debug issues.

! Change the hostname of your virtual machine

Configure the hostname for your virtual machine. You have chosen a username (e.g. `jde`) and have been assigned a domain for the course (e.g. `archidep2.ch`). Use a combination of both as the hostname for your server.

Tip

For example, if your username is `jde` and your assigned domain is `archidep2.ch`, your hostname should be `jde.archidep2.ch`. Make sure not to pick the same username/domain combination as someone else in the class.

```
$> sudo hostname jde.archidep8.ch
```

Also save your new hostname to the `/etc/hostname` file so that it will persist when you reboot the server:

```
$> echo "jde.archidep8.ch" | sudo tee /etc/hostname
```



The hostname is the name of your virtual server. It can be any URL. It often identifies a machine in an organization with the format `<machine-name>.<organization>.<tld>` (e.g. `unix-box.google.com`).

For the purposes of this course, we will be using prepared domains such as `archidep2.ch`, so it makes sense to use a subdomain corresponding to yourself (`jde.archidep2.ch`) as the hostname.

! Reboot the server

```
$> sudo reboot
```

Once the server has restarted (it might take a couple of minutes), check that you can still connect:

```
$> ssh jde@97.65.43.210
Welcome to Ubuntu 24.04 LTS
...
```

Also check that your hostname is correct:

```
$> hostname
jde.archidep2.ch
```

! Add swap space to your virtual server



The cloud servers used in this course do not have enough memory (RAM) to run/compile many things at once. But you can easily add **swap space** to solve this issue.

Swap space in Linux is used when there is no more available physical memory (RAM). If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space (on disk).

Adding 2 gigabytes of swap space should be enough for our purposes.

Run the following commands to make sure you disable any previous swap file you might have created during the exercises:

```
# (It's okay if this command produces an error.)
$> sudo swapoff /swapfile
$> sudo rm -f /swapfile
```

Use the following commands to create and mount a 2-gigabyte swap file:

```
$> sudo fallocate -l 2G /swapfile
$> sudo chmod 600 /swapfile
$> sudo mkswap /swapfile
Setting up swspace version 1, size = 2 GiB (2147479552 bytes)
no label, UUID=3c263053-41cc-4757-0000-13de0644cf97
$> sudo swapon /swapfile
```

You can verify that the swap space is correctly mounted by displaying available memory with the `free -h` command. You should see the `Swap` line indicating the amount of swap space you have added:

```
$> free -h
```

	total	used	free	shared	buff/cache	available
Mem:	914Mi	404Mi	316Mi	31Mi	193Mi	331Mi
Swap:	2.0Gi	200Mi	1.8Gi			

This swap space is temporary by default and will only last until you reboot your server. To make it permanent, you must tell your server to mount it on boot.

You can see the currently configured mounts with this command (the output may not be exactly the same):

```
$> cat /etc/fstab
```

```
# CLOUD_IMG: This file was created/modified by the Cloud Image build process
UUID=b1983cef-43a3-46ac-0000-b5e06a61c9fd / ext4 defaults,discard
UUID=0BC7-0000 /boot/efi vfat umask=0077 0 1
/dev/disk/cloud/azure_resource-part1 /mnt auto defaults,nofail,x-systemd
```



BE VERY CAREFUL TO EXECUTE THE FOLLOWING COMMAND EXACTLY AS IS.

Corrupting your `/etc/fstab` file can prevent your server from rebooting.

To make the swap space permanent, execute the following command to add the appropriate line to your server's `/etc/fstab` file:

```
$> echo "/swapfile none swap sw 0 0" | sudo tee -a /etc/fstab
```

This line tells your server to mount the swap file you have created as swap space on boot. You should see the new line at the end of the `/etc/fstab` file if you display its contents again:

```
$> cat /etc/fstab
```

```
# CLOUD_IMG: This file was created/modified by the Cloud Image build process
```

```

UUID=b1983cef-43a3-46ac-0000-b5e06a61c9fd      /      ext4      defaults,discard
UUID=0BC7-08EF  /boot/efi      vfat      umask=0077      0 1
/dev/disk/cloud/azure_resource-part1      /mnt      auto      defaults,nofail,x-systemd
/swapfile none swap sw 0 0

```

You can run the following command to check that you did not make any mistakes. It's okay if you have a couple of warnings about the swap file. These are expected since you've just added it and have not rebooted yet.

```

$> sudo findmnt --verify --verbose
/
[ ] target exists
[ ] FS options: discard,commit=30,errors=remount-ro
[ ] UUID=bf171e20-4158-4861-0000-1443ece8c413 translated to /dev/sda1
[ ] source /dev/sda1 exists
[ ] FS type is ext4
...
none
[W] non-bind mount source /swapfile is a directory or regular file
[ ] FS type is swap
[W] your fstab has been modified, but systemd still uses the old version;
    use 'systemctl daemon-reload' to reload

0 parse errors, 0 errors, 2 warnings

```

IF everything looks ok, reboot your server:

```
$> sudo reboot
```

Reconnect to your server over SSH and run the `free -h` command again. The swap space should still be enabled after reboot:

```

$> free -h

```

	total	used	free	shared	buff/cache	available
--	-------	------	------	--------	------------	-----------

Mem:	914Mi	404Mi	316Mi	31Mi	193Mi	331Mi
Swap:	2.0Gi	200Mi	1.8Gi			

Tip

You can also see the currently available swap space and how much is used with the `htop` command which shows it as the `Swp` bar at the top (you can quit it with `q` once it is open). For more information, see the [fstab Linux manpage](#).

! Register your Azure VM with us

Make a note of your virtual server's public IP address (the same IP address you used to connect to it with the `ssh` command).

Also run the following command **while connected to your server with SSH** to obtain your server's SSH host key fingerprints:

```
$> find /etc/ssh -name "*.pub" -exec ssh-keygen -lf {} \;
```

Just one more step, go back to the dashboard and:



Register your virtual server



When connecting to your server, we will match the public SSH key fingerprint it provides against the keys you are providing us to make sure we are connecting to your server and not an attacker's (man-in-the-middle).

The command above does a few things:

- The first `find` command finds all files named `*.pub` in the `/etc/ssh` directory, which contains the configuration files for the SSH

server running on your virtual server. These will be the public SSH host keys of your server, i.e. the keys it uses to sign the Diffie-Hellman key exchange parameters during the establishment of the SSH secure tunnel.

- The `-exec` option of the `find` command executes a command for each file that was found, with `{}` being the path to the file and `\;` a marker to mark the end of the command to execute.
- For each public SSH host key file, the `ssh-keygen -lf <file>` command is executed. The `ssh-keygen` command can not only generate new keys, but with the `-l` option, it can also show the fingerprints of the file specified with the `-f` (file) option.

Basically, the entire command will print the fingerprints of all public SSH host keys on your server.

What have I done?

You have used a popular Infrastructure-as-a-Service (IaaS) cloud service (Microsoft Azure) to set up a virtual machine for your own use. You are renting this virtual machine for a monthly fee (using your free education credits).

You have used what you have learned about the command line and SSH to connect to this virtual machine and perform some basic setup steps in preparation for future deployment exercises.

Troubleshooting

Here's a few tips about some problems you may encounter during this exercise.

🔥 I forgot to open some (or all) of the ports in the firewall

If you did not open the correct ports (80, 443, 3000 and 3001) during the initial configuration of your virtual server, you can go back to its network settings at any time and add the missing rules.

The screenshot shows the Azure portal interface for a virtual machine named 'ArchiDep'. The 'Network settings' tab is selected in the left sidebar. The main area displays the 'Network interface / IP configuration' for 'archidep876_z1 (primary) / ipconfig1 (primary)'. Below this, the 'Rules' section for the 'Network security group ArchiDep-nsg' is shown. A red box highlights the '+ Create port rule' button in the top right corner of the Rules section.

Priority	Name	Port	Protocol	Source	Destination	Action
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

As a reminder, you need to add inbound rules to open the following ports (if you haven't already):

- **Service:** HTTP, **Action:** Allow, **Name:** HTTP
- **Service:** HTTPS, **Action:** Allow, **Name:** HTTPS
- **Service:** Custom, **Destination port ranges:** 3000, **Protocol:** TCP, **Action:** Allow, **Name:** Port3000
- **Service:** Custom, **Destination port ranges:** 3001, **Protocol:** TCP, **Action:** Allow, **Name:** Port3001



Azure complains that my RSA key is too short

Azure requires that SSH keys of type RSA have at least 2048 bits. If your existing key is not accepted by Azure when pasting it in the administrator account settings of your virtual server later, you may need to generate a new one with enough bits:

```
ssh-keygen -m PEM -t rsa -b 4096
```



ATTENTION! If you already have an RSA key, this command will ask you if you want to overwrite it with the new one. If you do, the old key will be **PERMANENTLY LOST**. (You will need to put your public key on GitHub again and everywhere else you may have used it.)

[↑ Back to top](#)