

AFTER AZ-900

You passed the exam. *Now build it.*

Thirty days of hands on Azure labs. The same basics AZ-900 covered, this time in the CLI, with the security reasoning behind every click.

18 labs

1 capstone

About 90 minutes a day

CLI and portal, side by side

Prepared for _____



MICHAEL ADEYANJU

michaeladeyanju.com

AZ-900 taught the words. *This month teaches the hands.*

Five labs a week, about ninety minutes each. Weekends are for the write up and catching up. Every lab ends with proof in your GitHub repo and one question to answer for your mentor.

BEFORE DAY 01

- **An Azure subscription you control.** The free account works. Read the current credit and free services terms at azure.microsoft.com/free.
- **Azure Cloud Shell (Bash)** in the portal, or the Azure CLI installed locally. Commands here assume Bash.
- **A GitHub repo** called `azure-security-labs`. One folder per day.
- **VS Code** with the Bicep extension, for Day 02 and the capstone.
- **An authenticator app** on your phone for MFA.

THE LAB ANATOMY

- **Steps, then In the portal.** Each lab is done in the CLI first, then the next page walks the same lab in the portal, with a drawing to follow.
- **Break it.** A deliberate mistake or attacker view. This is where the learning is.
- **Proof.** What goes in your repo. Never commit keys, tokens or passwords.
- **Clean up.** What to keep and what to delete.
- **Mentor question.** Answer it in two or three sentences in your notes.

FOUR RULES THAT PROTECT YOUR WALLET

1. Budget alert before anything else. 2. One resource group per week, deleted at the end of the week. 3. Deallocate VMs every evening: a stopped VM can still bill, a deallocated one does not bill for compute. 4. Use the smallest sizes in these labs and never enable paid Defender plans.

VARIABLES USED THROUGHOUT

```
LOC=southafricanorth      # or the closest region your subscription allows
ME=$(curl -s ifconfig.me)  # your public IP, for firewall rules
SUB=$(az account show --query id -o tsv)
```

Four weeks.

Each one builds on the last.

Week 1 is identity and governance, because everything else depends on it. Week 2 is networks and servers. Week 3 is data and the identities workloads use. Week 4 is seeing what happened, then building it all again from code.

WEEK 1 • FOUNDATIONS YOU CAN TOUCH • RG-LAB-W1

01

Set up like a professional

02

One resource, three ways

03

Entra ID users and groups

04

RBAC and scope

05

Azure Policy guardrails

WEEK 2 • NETWORKS AND COMPUTE • RG-LAB-W2

06

Plan and build a VNet

07

First VM, the safe way

08

Lose the public IP

09

Peering and traffic tests

10

Hunt the exposure

WEEK 3 • DATA AND WORKLOAD IDENTITY • RG-LAB-W3

11

Storage done right

12

Key Vault

13

Managed identity

14

Private endpoints

15

Recovery and locks

WEEK 4 • WATCH, DETECT, PROVE • RG-LAB-W4

16

Logs and KQL

17

Defender for Cloud

18

Alerts and a mini incident

19

Capstone build

20

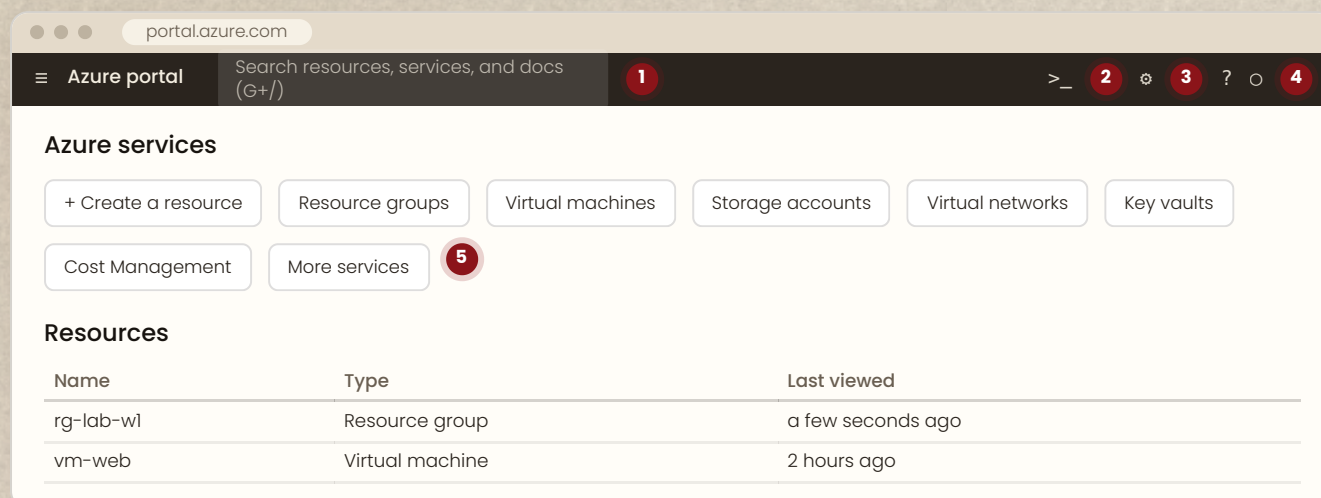
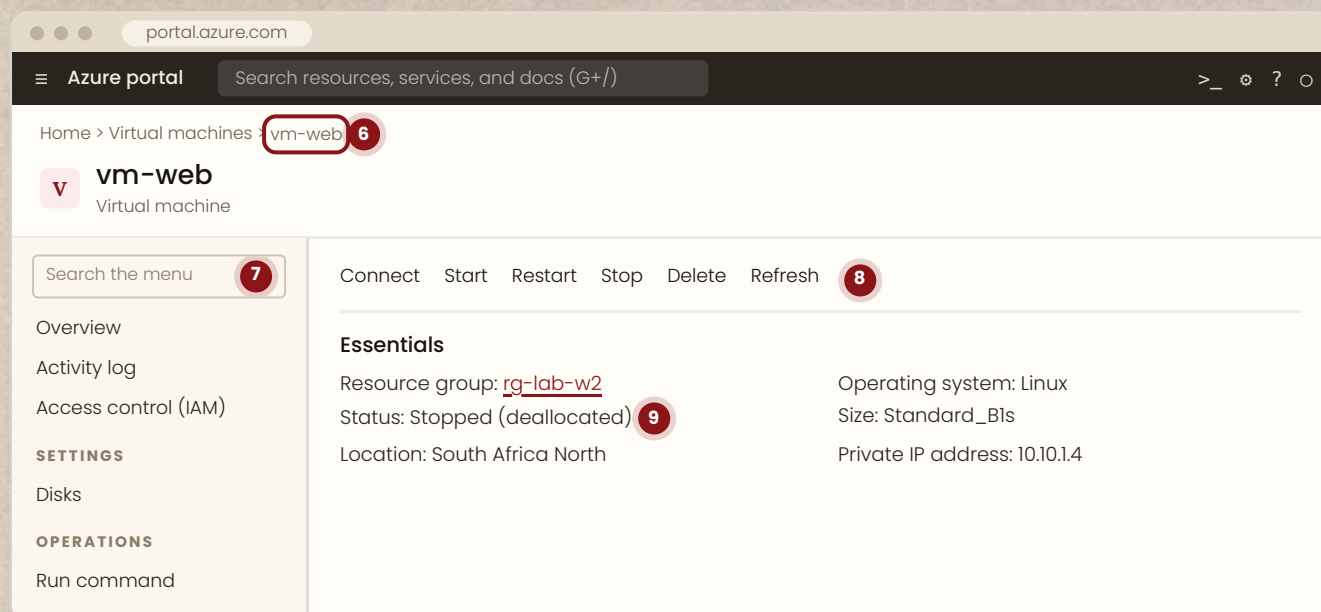
Capstone review

BY DAY 20 YOU CAN

Deploy a small, locked down Azure environment from one Bicep command, explain every control in it, and show the logs that prove it works.

Nine places to know.

The rest is search.



Illustrations, simplified. The live portal changes often, so labels and positions may differ slightly.

- 01 Global search.** The fastest way to anything. Type a service ("Key vaults") or a resource name ("vm-web").
- 02 Cloud Shell.** A Bash terminal in the browser with the Azure CLI already signed in.
- 03 Settings.** Switch directory or subscription here when you have more than one.
- 04 Your account.** Who you are signed in as. Check it when testing as labreader.
- 05 Services.** Every lab starts from a service list. "+ Create a resource" is the marketplace.
- 06 Breadcrumb.** Where you are. Click any part to go back up a level.
- 07 Resource menu.** Every resource has one. It has a search box, so you never need to scroll.
- 08 Command bar.** Actions for this resource. Stop in the portal also deallocates a VM.
- 09 Essentials.** The summary every resource opens on: group, region, status, key settings.

01

60 min

Set up like a professional. *Before you build anything.*

A subscription you will not regret: MFA on, a budget alert, a naming habit, and your first tagged resource group.

STEPS

01 Turn on MFA for your own account. Check Entra ID, then Properties, then Manage security defaults. Note whether security defaults are on.

02 Create a budget. Cost Management, then Budgets. Set it low on purpose, with alerts at 50, 90 and 100 percent. The point is the email.

03 Open Cloud Shell and confirm where you are.

```
az account show -o table
az account list-locations --query "[].name" -o tsv | head -20
```

04 Create the week's resource group with tags you will reuse all month.

```
az group create -n rg-lab-w1 -l $LOC \
--tags owner=<yourname> purpose=lab expires=week1
```

05 Write your naming rule in the repo README: `rg-`, `vnet-`, `snet-`, `nsg-`, `vm-`, `st`, `kv-`, `law-`.

BREAK IT

Find out the difference between a stopped and a deallocated VM, and which one still bills for compute. One sentence, in your own words.

PROOF FOR YOUR REPO

Screenshot of the budget alert settings. Output of `az group show -n rg-lab-w1`.

CLEAN UP

Keep `rg-lab-w1` for the week.

MENTOR QUESTION

Who receives the budget email, and what exactly do you do in the first ten minutes after it arrives?

A budget first. Then everything else.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Cost Management | Budgets >

Create budget
Cost Management

Create a budget **Set alerts**

Alert conditions 3

Type	% of budget	Amount
Actual	50	5
Actual	90	9
Actual	100	10

Alert recipients (email)

Email 4

5 Create Previous Cancel

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Search "Cost Management" in the top bar, open it, and choose **Budgets** in the left menu.
- 02** + **Add**. Check the scope is your subscription. Name it **budget-lab**, reset period Monthly, a low amount. Next.
- 03** Add three alert conditions, all of type Actual, at 50, 90 and 100 percent.
- 04** Alert recipients: your email address.
- 05** **Create**. The budget now appears in the Budgets list.
- 06** **MFA**: search Microsoft Entra ID, then Overview, Properties, **Manage security defaults**.
- 07** **Resource group**: search Resource groups, + **Create**, name **rg-lab-w1**, pick your region. On the **Tags** tab add owner, purpose and expires. Review + create.

CHECK IT WORKED

budget-lab is listed under **Budgets**, and **rg-lab-w1** shows three tags on its **Overview**.

02

90 min

One resource, three ways. *Same API underneath.*

The portal, the CLI and a template all call Azure Resource Manager. Seeing that once changes how you think about security.

STEPS

01 Portal. Create a storage account in rg-lab-w1. On the Review page, open "View automation template" and read it before you click Create.

02 CLI. Create a second one. Names must be globally unique, lowercase, no dashes.

```
az storage account create -n st<initials>cli01 -g rg-lab-w1 -l $LOC --sku Standard_LRS
```

03 Bicep. Save this as `day02/main.bicep` and deploy it.

```
param location string = resourceGroup().location
resource st 'Microsoft.Storage/storageAccounts@2023-05-01' = {
  name: 'st${uniqueString(resourceGroup().id)}'
  location: location
  sku: { name: 'Standard_LRS' }
  kind: 'StorageV2'
}
```

04 Deploy, then compare all three.

```
az deployment group create -g rg-lab-w1 -f day02/main.bicep
az storage account list -g rg-lab-w1 -o table
```

05 Open the Activity log for the resource group. Find all three create operations and who made them.

BREAK IT

Run the Bicep deployment a second time. What changed? Then switch the SKU to Standard_GRS and run `az deployment group what-if` before deploying.

PROOF FOR YOUR REPO

Commit `main.bicep` and the what-if output.

CLEAN UP

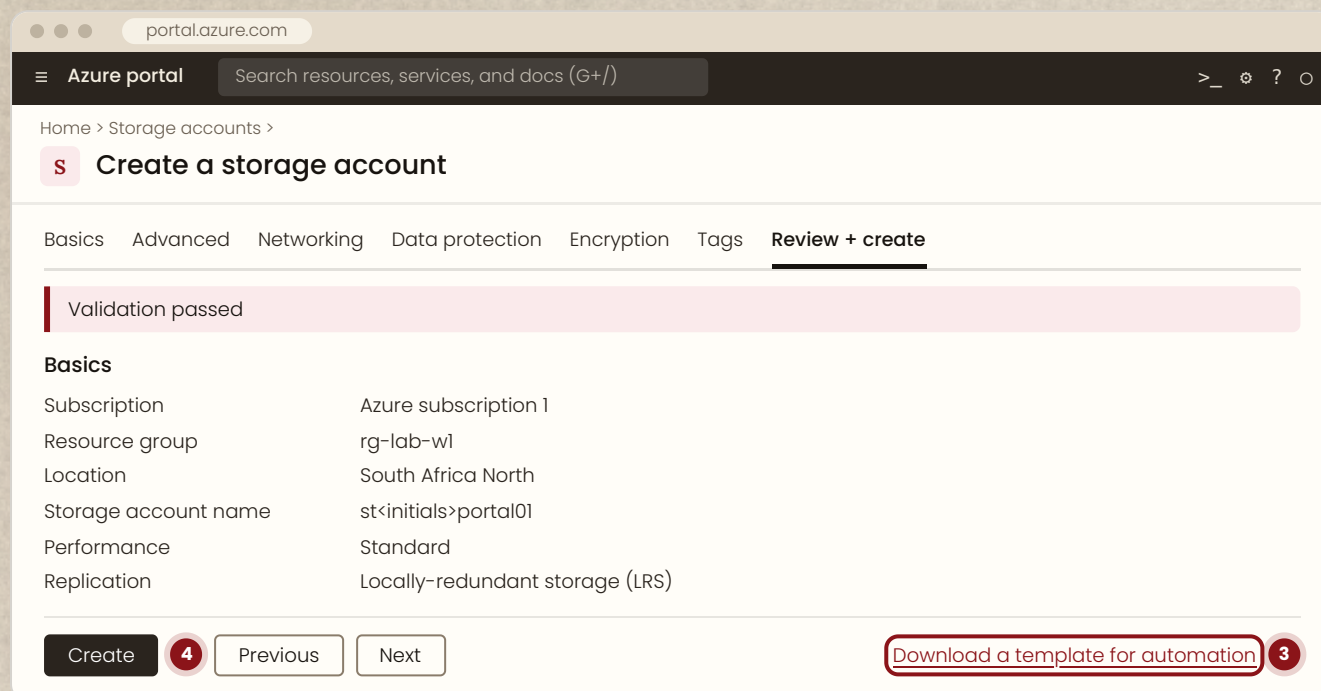
Delete the portal and CLI storage accounts. Keep the Bicep one.

MENTOR QUESTION

Why do security teams prefer templates over portal clicks, even for small changes?

Click Create.

Read what it sends first.



portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags **Review + create**

Validation passed

Basics

Subscription	Azure subscription 1
Resource group	rg-lab-w1
Location	South Africa North
Storage account name	st<initials>portal01
Performance	Standard
Replication	Locally-redundant storage (LRS)

Create **4** Previous Next **3** Download a template for automation

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Search "Storage accounts", then + Create.
- 02** **Basics:** rg-lab-w1, a unique lowercase name, your region, Standard, LRS. Leave the other tabs on their defaults and go to **Review + create**.
- 03** **Download a template for automation.** Read the JSON. This is exactly what Create sends to Resource Manager.
- 04** Go back and click Create.
- 05** Open rg-lab-w1, then Activity log. Find the create operation for each of the three accounts and who made it.
- 06** Open Settings, then Deployments in the resource group to see your Bicep deployment and its inputs.

CHECK IT WORKED

Three storage accounts in rg-lab-w1, and three create entries in its Activity log.

03

75 min

Identity first.

Users and groups.

In the cloud, identity is the perimeter. Create a test identity and watch what it can and cannot do.

STEPS

01 Find your tenant domain: Entra ID, then Overview, then Primary domain. It ends in `onmicrosoft.com`.

02 Create a test user. Generate the temporary password, do not reuse one of yours.

```
az ad user create --display-name "Lab Reader" \  
  --user-principal-name labreader@<domain> \  
  --password "$(openssl rand -base64 18)Aa1!" --force-change-password-next-sign-in true
```

03 Create a group and add the user.

```
az ad group create --display-name grp-lab-readers --mail-nickname grp-lab-readers  
UID=$(az ad user show --id labreader@<domain> --query id -o tsv)  
az ad group member add --group grp-lab-readers --member-id $UID
```

04 Reset the password in the portal so you know it, then sign in as labreader in a private browser window. What can you see?

05 Look at the sign-in logs for labreader in Entra ID. Note the IP, app and result.

BREAK IT

As labreader, try to create a resource group. Copy the full error. It names the exact permission missing. Find that action string.

PROOF FOR YOUR REPO

Screenshot of the authorisation error with the action string highlighted.

CLEAN UP

Keep the user and group. You need them on Days 4 and 18.

MENTOR QUESTION

What is the difference between an Entra ID role and an Azure RBAC role? Give one example of each.

Make a test user.

Then become them.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Microsoft Entra ID | Users >

Create new user

Basics Properties Assignments Review + create

Identity

User principal name * labreader @ <yourtenant>.onmicrosoft.com

Mail nickname ☒ Derive from user principal name

Display name * Lab Reader

Password * [Copy](#)

☒ Auto-generate password

Account enabled ☐

Review + create < Previous Next: Properties >

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Search "Microsoft Entra ID". Open **Users** under Manage, then **+ New user**, then **Create new user**.
- 02** User principal name **labreader**, your onmicrosoft.com domain from the dropdown. Display name Lab Reader.
- 03** Keep **Auto-generate password** ticked and copy it now. It is shown once.
- 04** **Review + create**, then **Create**.
- 05** **Groups**, then **+ New group**. Type Security, name **grp-lab-readers**. Under Members, add Lab Reader. Create.
- 06** Open a private window at portal.azure.com and sign in as labreader. Set a new password when asked.
- 07** Back as yourself: Users, Lab Reader, **Sign-in logs**. Note the IP, application and result.

CHECK IT WORKED

Lab Reader is a member of grp-lab-readers, and the sign-in shows as Success in the log.

04

90 min

Least privilege. At the right scope.

Azure RBAC is role plus principal plus scope. Get one wrong and you give away too much.

STEPS

01 Grant Reader to the group, on the resource group only.

```
RGID=$(az group show -n rg-lab-w1 --query id -o tsv)
GID=$(az ad group show -g grp-lab-readers --query id -o tsv)
az role assignment create --assignee-object-id $GID \
  --assignee-principal-type Group --role Reader --scope $RGID
```

02 Sign in as labreader again. Which resource groups are visible now, and why?

03 Audit who has what across the subscription.

```
az role assignment list --all --query "[].\n{who:principalName,role:roleDefinitionName,scope:scope}" -o table
```

04 Write a custom role in `day04/vm-operator.json`, then create it with `az role definition create --role-definition @day04/vm-operator.json`.

```
{
  "Name": "Lab VM Operator",
  "Description": "Start, restart and deallocate VMs only.",
  "Actions": ["Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action"],
  "AssignableScopes": ["/subscriptions/<sub-id>"]
}
```

BREAK IT

Give labreader Contributor on the group. As labreader, try to grant yourself Owner. Why does Azure refuse?

PROOF FOR YOUR REPO

`vm-operator.json` plus a paragraph on scope inheritance.

CLEAN UP

Remove the Contributor assignment. Keep the custom role.

MENTOR QUESTION

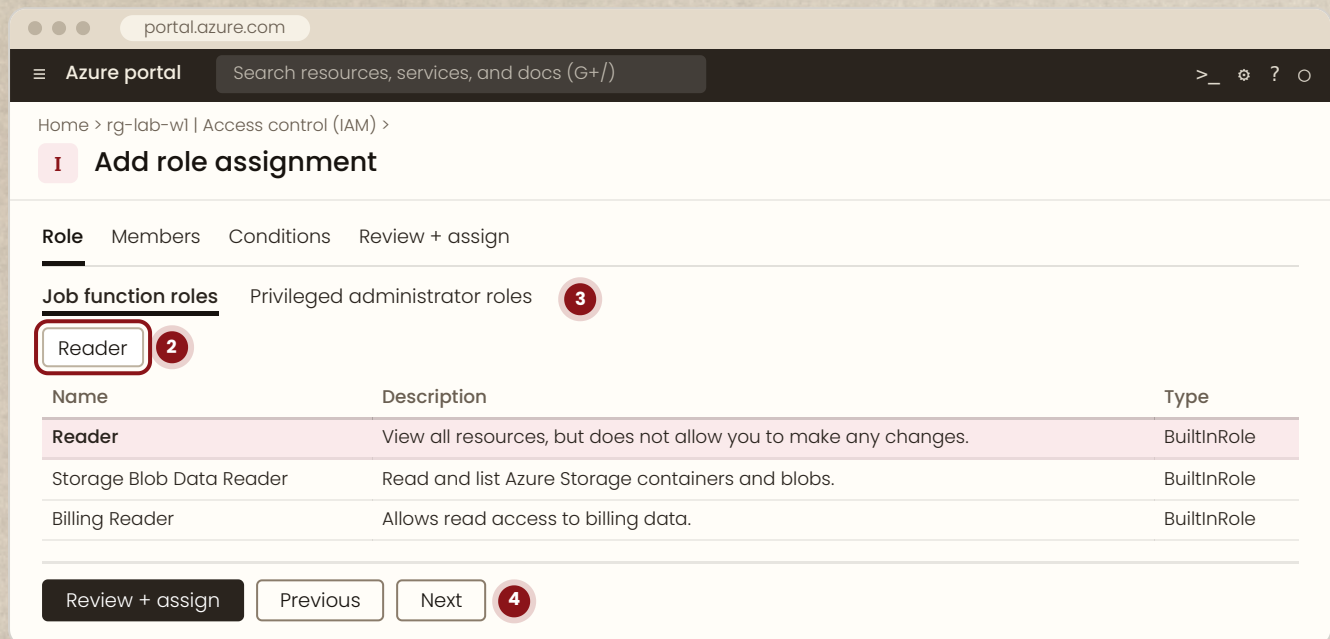
A developer asks for Owner on the subscription to deploy one app. What do you offer instead, and why?

MICHAEL ADEYANJU

michaeladeyanju.com

Role, member, scope.

Three tabs, three decisions.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Open rg-lab-w1, then Access control (IAM), then + Add, then Add role assignment.
- 02** Role tab: search Reader and select that row.
- 03** Notice the second tab. Owner and Contributor live under Privileged administrator roles, kept apart on purpose.
- 04** Next. Members tab: User, group, or service principal, then + Select members, pick grp-lab-readers.
- 05** Review + assign.
- 06** Check access tab: search Lab Reader to see what they can do and where it was granted.
- 07** Custom role: on the subscription, Access control (IAM), + Add, Add custom role, Start from JSON, upload vm-operator.json.

CHECK IT WORKED

Role assignments lists grp-lab-readers as Reader with scope "This resource".

05

90 min

Guardrails.

Stop mistakes before they land.

RBAC decides who can act. Azure Policy decides what is allowed to exist. You need both.

STEPS

01 Find two built-in policies by display name.

```
az policy definition list --query "[?displayName=='Allowed locations'].name" -o tsv
az policy definition list --query "[?displayName=='Require a tag on resources'].name" -o tsv
```

02 Assign Allowed locations to the resource group.

```
az policy assignment create -n only-my-region --scope $RGID \
--policy <id-from-step-1> \
--params '{"listOfAllowedLocations":{"value":["$LOC"]}}'
```

03 Assign Require a tag for the tag `owner`.

```
az policy assignment create -n require-owner-tag --scope $RGID \
--policy <id-from-step-1> --params '{"tagName":{"value":"owner"}}'
```

04 Wait 10 to 20 minutes, then try to create a storage account in another region, and one without an owner tag. Both should be denied.

05 Check compliance.

```
az policy state summarize --resource-group rg-lab-w1
```

BREAK IT

The Bicep storage account from Day 02 has no owner tag. Policy does not delete it. Find it in the compliance view and decide what you would do in a real company.

PROOF FOR YOUR REPO

Both deny errors and the compliance summary. Plus your Week 1 write up: what you learned setting up Azure properly.

CLEAN UP

End of week. `az group delete -n rg-lab-w1 --yes --no-wait`. Keep the user, group and custom role.

MENTOR QUESTION

Audit or Deny: when would you choose each, and what goes wrong if you choose Deny on day one?

Pick the scope.

Pick the rule. Enforce it.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Policy | Assignments >

P Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope

Scope * Azure subscription 1/rg-lab-wl ... 2

Exclusions Optionally select resources to exclude ...

Basics

Policy definition * Allowed locations ... 3

Assignment name * only-my-region

Policy enforcement Enabled Disabled 5

Review + create Cancel Previous Next

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Search "Policy". Under Authoring choose **Assignments**, then **Assign policy**.
- 02 **Scope**: click the three dots, pick your subscription and rg-lab-wl.
- 03 **Policy definition**: click the three dots, search Allowed locations, Add.
- 04 **Parameters tab**: choose your region in Allowed locations.
- 05 **Policy enforcement Enabled** means non-compliant requests are denied. Review + create, then Create.
- 06 **Repeat** with Require a tag on resources, Tag Name **owner**.
- 07 **Policy, then Compliance**. Give it 15 to 30 minutes, then filter to rg-lab-wl.

CHECK IT WORKED

Both assignments are listed, and a create in another region fails with a policy error naming only-my-region.

06

75 min

Plan the network. Then build it.

Re-addressing a live network is painful. Plan the address space on paper first, then build exactly that.

STEPS

01 On paper: `vnet-lab` 10.10.0.0/16 with `snet-web` 10.10.1.0/24, `snet-app` 10.10.2.0/24, `snet-data` 10.10.3.0/24. How many usable addresses does Azure give you in a /24, and why not 254?

02 Build it.

```
az group create -n rg-lab-w2 -l $LOC --tags owner=<yourname> purpose=lab
az network vnet create -g rg-lab-w2 -n vnet-lab --address-prefix 10.10.0.0/16 \
  --subnet-name snet-web --subnet-prefix 10.10.1.0/24
az network vnet subnet create -g rg-lab-w2 --vnet-name vnet-lab \
  -n snet-app --address-prefixes 10.10.2.0/24
az network vnet subnet create -g rg-lab-w2 --vnet-name vnet-lab \
  -n snet-data --address-prefixes 10.10.3.0/24
```

03 One NSG per subnet, attached at the subnet. Repeat for app and data.

```
az network nsg create -g rg-lab-w2 -n nsg-web
az network vnet subnet update -g rg-lab-w2 --vnet-name vnet-lab \
  -n snet-web --network-security-group nsg-web
```

04 Read every default rule and write what each one allows.

```
az network nsg rule list -g rg-lab-w2 --nsg-name nsg-web --include-default -o table
```

BREAK IT

Try to add a subnet 10.10.1.128/25. Read the error. Then explain why overlapping ranges also break peering later.

PROOF FOR YOUR REPO

A diagram of the network (draw.io or Excalidraw) committed as `day06/network.png`.

CLEAN UP

Keep everything for the week.

MENTOR QUESTION

What does the default rule `AllowVnetInBound` really allow, and why does that matter once networks are peered?

Address space first. Subnets second.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Virtual networks >

Create virtual network

Basics Security **IP addresses** Tags Review + create

10.10.0.0/16 10.10.0.0 to 10.10.255.255 · 65,536 addresses 2

+ Add a subnet 3

Subnets	IP address range	Size	NAT gateway
snet-web	10.10.1.0 to 10.10.1.255	/24 (256 addresses)	-
snet-app	10.10.2.0 to 10.10.2.255	/24 (256 addresses)	-
snet-data	10.10.3.0 to 10.10.3.255	/24 (256 addresses)	-

Review + create < Previous Next >

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Search "Virtual networks", + Create. Basics: Create new resource group `rg-lab-w2`, name `vnet-lab`, your region.
- 02** IP addresses tab: set the address space to 10.10.0.0/16.
- 03** Delete the default subnet, then + Add a subnet three times: snet-web, snet-app, snet-data.
- 04** Review + create, then Create.
- 05** Search "Network security groups", + Create nsg-web in rg-lab-w2. Repeat for nsg-app and nsg-data.
- 06** Open nsg-web, Settings, Subnets, + Associate: vnet-lab and snet-web. Repeat for the others.
- 07** nsg-web, Inbound security rules. Read the three default rules at priorities 65000, 65001 and 65500.

CHECK IT WORKED

vnet-lab shows three subnets, each with its own network security group in the Subnets list.

07

90 min

Your first VM. *Built the safe way.*

Most cloud compromises start with a server exposed to the whole internet. Build one that is only reachable from you.

STEPS

- 01 Create the VM** with SSH keys and no NIC level NSG, so the subnet NSG is the only one in play.

```
az vm create -g rg-lab-w2 -n vm-web --image Ubuntu2204 --size Standard_B1s \
--vnet-name vnet-lab --subnet snet-web --nsg "" \
--admin-username azureuser --generate-ssh-keys --public-ip-sku Standard
```

- 02 Allow SSH from your IP only.**

```
az network nsg rule create -g rg-lab-w2 --nsg-name nsg-web -n allow-ssh-me \
--priority 100 --direction Inbound --access Allow --protocol Tcp \
--source-address-prefixes $ME/32 --destination-port-ranges 22
```

- 03 SSH in and look around.** Install nginx, then list what is listening.

```
ssh azureuser@<public-ip>
sudo apt update && sudo apt install -y nginx
ss -tlnp
```

- 04 Check the effective rules** for the VM NIC in the portal: Networking, then Effective security rules.

BREAK IT

Switch your laptop to a phone hotspot so your IP changes. Try SSH again. Then try `curl http://<public-ip>`. Explain both results.

PROOF FOR YOUR REPO

Screenshot of SSH working from your IP and timing out from the hotspot.

CLEAN UP

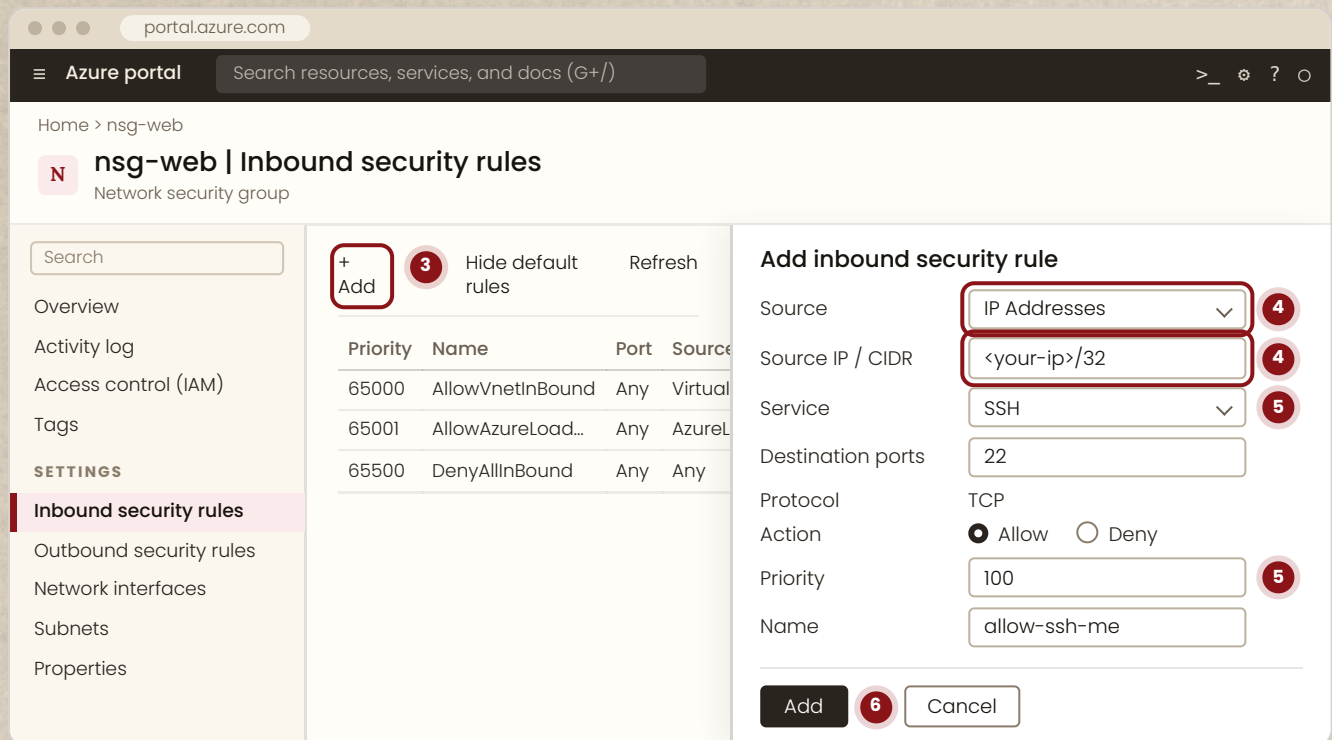
Deallocate every evening: `az vm deallocate -g rg-lab-w2 -n vm-web`.

MENTOR QUESTION

Why is SSH key login safer than a password, and what is still risky about port 22 open to one IP?

One rule.

One IP. One port.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Create the VM:** Virtual machines, + Create, Azure virtual machine. rg-lab-w2, **vm-web**, Ubuntu Server 22.04 LTS, Standard_B1s, SSH public key, **Public inbound ports None**.
- 02 Networking tab:** vnet-lab, snet-web, NIC network security group **None**. Create, and download the private key when asked.
- 03 Open nsg-web, Inbound security rules, + Add.**
- 04 Source IP Addresses**, then your public IP with **/32**. Search "what is my IP" if unsure.
- 05 Service SSH** fills in port 22. Action Allow, Priority 100.
- 06 Name it allow-ssh-me**, then Add.
- 07 vm-web, Networking, Network settings:** open the effective security rules for the NIC and confirm.

CHECK IT WORKED

SSH works from your IP. The VM Overview shows Status "Stopped (deallocated)" after you click Stop at the end of the day.

08

75 min

Lose the public IP. *Keep the access.*

The safest management port is the one that does not exist. Manage the server with no public IP at all.

STEPS

01 Run a command without SSH, through the Azure control plane.

```
az vm run-command invoke -g rg-lab-w2 -n vm-web \  
--command-id RunShellScript --scripts "hostname; ss -tlnp"
```

02 Remove the public IP from the NIC, then delete it. These are the default names `az vm create` used.

```
az network nic ip-config update -g rg-lab-w2 --nic-name vm-webVMNic \  
-n ipconfigvm-web --remove publicIpAddress \  
az network public-ip delete -g rg-lab-w2 -n vm-webPublicIP
```

03 Delete the `allow-ssh-me` rule. It now protects nothing, and stale rules are how exposures come back.

04 Run the `run-command` again. It still works. Write down why.

05 Read about [Azure Bastion](#) and just-in-time VM access. Note what each one costs and when you would pick it.

BREAK IT

Think like an attacker. Someone has Contributor on this resource group but no SSH key. Can they run code on your VM? Which permission makes it possible?

PROOF FOR YOUR REPO

The `run-command` output and your answer to Break it.

CLEAN UP

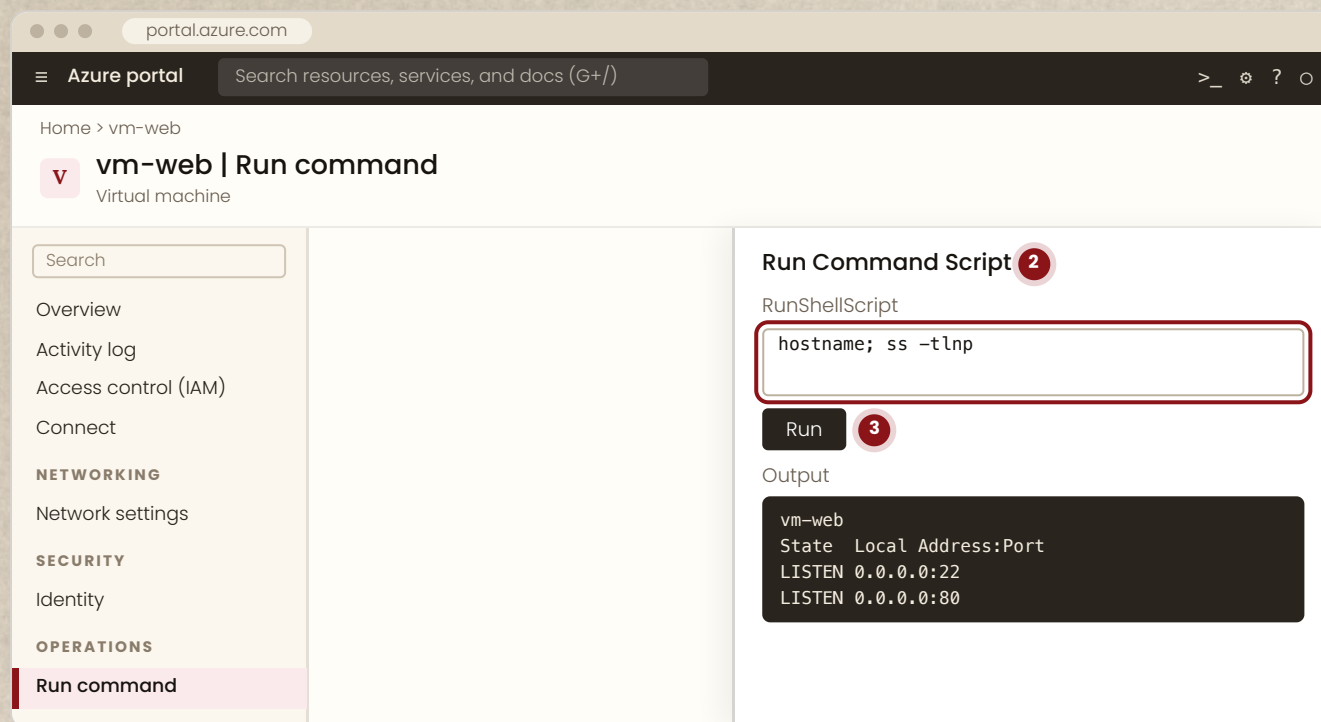
Deallocate the VM.

MENTOR QUESTION

Name three ways to reach a VM that has no public IP, and the trade-off of each.

No SSH needed.

That is the lesson and the risk.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Open **vm-web**. Under Operations choose **Run command**.
- 02** Choose **RunShellScript**. A script panel opens on the right.
- 03** Type `hostname; ss -tlnp` and click **Run**. Output appears after a short wait.
- 04** Remove the public IP: Networking, Network settings, open the network interface, IP configurations, the ipconfig, then untick Associate public IP address. Save.
- 05** Search "Public IP addresses", open **vm-webPublicIP**, Delete.
- 06** **nsg-web**, Inbound security rules: delete **allow-ssh-me**.
- 07** **vm-web**, **Connect**: read the options and note which ones need a public IP.

CHECK IT WORKED

vm-web Overview shows no public IP, and Run command still returns output.

09

90 min

Two networks. Prove what can talk.

Never assume traffic is blocked. Test it, record it, then change one rule and test again.

STEPS

01 Build a second network and a VM with no public IP.

```
az network vnet create -g rg-lab-w2 -n vnet-b --address-prefix 10.20.0.0/16 \
  --subnet-name snet-a --subnet-prefix 10.20.1.0/24
az vm create -g rg-lab-w2 -n vm-b --image Ubuntu2204 --size Standard_B1s \
  --vnet-name vnet-b --subnet snet-a --public-ip-address "" \
  --admin-username azureuser --generate-ssh-keys
```

02 Peer both directions.

```
az network vnet peering create -g rg-lab-w2 -n lab-to-b \
  --vnet-name vnet-lab --remote-vnet vnet-b --allow-vnet-access
az network vnet peering create -g rg-lab-w2 -n b-to-lab \
  --vnet-name vnet-b --remote-vnet vnet-lab --allow-vnet-access
```

03 From vm-web, use run-command to `ping` and `curl` the private IP of vm-b. Record the result.

04 Ask Network Watcher what is allowed, without sending real traffic.

```
az network watcher test-ip-flow -g rg-lab-w2 --vm vm-b --direction Inbound \
  --protocol TCP --local <vm-b-ip>:22 --remote 10.10.1.4:50000
```

05 Add a deny rule on vm-b's NSG for traffic from 10.10.1.0/24, then repeat steps 3 and 4.

BREAK IT

Peering is not transitive. If vnet-c peers only with vnet-b, can vm-web reach it? Predict the answer first, then check the docs or test it.

PROOF FOR YOUR REPO

Before and after output of test-ip-flow and the curl test.

CLEAN UP

Delete vm-b and vnet-b after today. Deallocate vm-web.

MENTOR QUESTION

Why do default NSG rules make two peered networks wide open to each other?

Ask the network.

Do not guess.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Network Watcher

Network Watcher | IP flow verify

Search

Overview

MONITORING

Topology

Connection monitor

NETWORK DIAGNOSTIC T...

IP flow verify

NSG diagnostics

Next hop

Effective security rules

Connection troubleshoot

Packet capture

Virtual machine * vm-b

Network interface vm-bVMNic

Protocol ☒ TCP ☐ UDP

Direction ☒ Inbound ☐ Outbound

Local IP address : port 10.20.1.4 22

Remote IP address : port 10.10.1.4 50000

Verify IP flow

Access allowed - Security rule: AllowVnetInBound

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Build **vnet-b** (10.20.0.0/16, snet-a 10.20.1.0/24) and **vm-b** with Public IP None, as on Days 06 and 07.
- 02** **vnet-lab**, **Settings**, **Peerings**, + **Add**. One form creates both directions: remote link **b-to-lab**, local link **lab-to-b**, remote network vnet-b. Add.
- 03** Wait until both **peerings** show **Connected**.
- 04** Search "**Network Watcher**", then **IP flow verify**. Choose **vm-b**, **TCP**, **Inbound**.
- 05** **Local**: **vm-b** private IP and port **22**. **Remote**: **10.10.1.4** and any high port.
- 06** **Verify IP flow** and read which rule made the decision.
- 07** Add the **deny rule** on **vm-b**'s **NSG** for **10.10.1.0/24**, then verify again.

CHECK IT WORKED

The first result names **AllowVnetInBound**. After your rule, the result is **Access denied** and names your rule.

10

90 min

Hunt the exposure. *Like an auditor.*

Real estates have hundreds of NSGs. Nobody checks them one by one. Query the whole subscription instead.

STEPS

- 01 Plant a bad rule** on purpose: RDP open to the internet.

```
az network nsg rule create -g rg-lab-w2 --nsg-name nsg-web -n bad-rdp \
--priority 200 --access Allow --protocol Tcp --source-address-prefixes "*" \
--destination-port-ranges 3389
```

- 02 Query every NSG** in the subscription with Resource Graph.

```
az extension add -n resource-graph
az graph query -q "Resources | where type =~ 'microsoft.network/networksecuritygroups'
| mv-expand r = properties.securityRules
| where r.properties.access == 'Allow' and r.properties.direction == 'Inbound'
| where r.properties.sourceAddressPrefix in ('*', '0.0.0.0/0', 'Internet')
| project nsg=name, rule=tostring(r.name), port=tostring(r.properties.destinationPortRange)"
```

- 03 Open Defender for Cloud** and look for the same finding in Recommendations. It can take hours to show up. Note the delay.

- 04 Fix it.** Delete the rule, rerun the query, confirm it is gone.

BREAK IT

Extend the query to also catch port ranges such as `0-65535` or `*`, and rules that list several ports in `destinationPortRanges`.

PROOF FOR YOUR REPO

The query saved as `day10/open-inbound.kql`. Plus your Week 2 write up.

CLEAN UP

End of week. `az group delete -n rg-lab-w2 --yes --no-wait`.

MENTOR QUESTION

Why is a saved query better audit evidence than a screenshot?

One query. Every NSG at once.

The screenshot shows the Azure portal interface. At the top, the browser address bar shows 'portal.azure.com'. The portal header includes the 'Azure portal' logo and a search bar. Below the header, the 'Resource Graph Explorer' is open. On the left, there's a sidebar with 'Search tables' and a list of categories and resource types. The main area shows a query editor with a query that filters for network security groups with inbound rules allowing traffic from the Internet on port 3389. The 'Run query' button is highlighted with a red circle and the number 3. Below the query, the results are displayed in a table with columns 'nsg', 'rule', and 'port'. One result is shown: 'nsg-web', 'bad-rdp', and '3389'. The 'Results' label is highlighted with a red circle and the number 4. The 'Download as CSV' button is highlighted with a red circle and the number 5.

Search tables

Home > Resource Graph Explorer

Categories: Resources, Security resources, Policy resources, Advisor resources

Resource types: microsoft.network, microsoft.compute, microsoft.storage

Query: Resources | where type =~ 'microsoft.network/networksecuritygroups' | mv-expand r = properties.securityRules | where r.properties.access == 'Allow' and r.properties.direction == 'Inbound' | where r.properties.sourceAddressPrefix in ('*', '0.0.0.0/0', 'Internet') | project nsg=name, rule=tostring(r.name), port=tostring(r.properties.destinationPortRange)

Run query (3) Save as Download as CSV (5)

Results (4)

nsg	rule	port
nsg-web	bad-rdp	3389

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Plant the bad rule: nsg-web, Inbound security rules, + Add. Source Any, port 3389, Allow, Priority 200, name bad-rdp. Read the warning the portal shows you.
- 02 Search "Resource Graph Explorer".
- 03 Paste the query from the lab and click Run query.
- 04 Read the results. One row per exposed rule, across every NSG you can see.
- 05 Download as CSV for evidence. Save as keeps the query for next time.
- 06 Defender for Cloud, Recommendations: search for management ports and compare. Note how long it took to appear.
- 07 Delete bad-rdp and run the query again.

CHECK IT WORKED

The second run returns no rows.

11

90 min

Storage done right. *Private by default.*

Public storage is one of the most common cloud leaks. Learn what safe looks like, then make it unsafe on purpose.

STEPS

01 Rebuild Week 2 in rg-lab-w3 with one script you write: VNet, three subnets, NSGs, vm-web with no public IP. Commit it as `day11/base.sh`.

02 Create a hardened storage account.

```
SA=st<initials>$RANDOM
az storage account create -n $SA -g rg-lab-w3 -l $LOC --sku Standard_LRS \
  --min-tls-version TLS1_2 --allow-blob-public-access false --https-only true
```

03 Give yourself data access with RBAC, then upload with your identity, not a key.

```
SAID=$(az storage account show -n $SA --query id -o tsv)
az role assignment create --assignee <your-upn> --role "Storage Blob Data Contributor" --scope $SAID
az storage container create --account-name $SA -n docs --auth-mode login
echo hello > hello.txt
az storage blob upload --account-name $SA -c docs -f hello.txt -n hello.txt --auth-mode login
```

04 Share it safely: a read only user delegation SAS that expires in one hour.

```
az storage blob generate-sas --account-name $SA -c docs -n hello.txt --permissions r \
  --expiry $(date -u -d '+1 hour' +%Y-%m-%dT%H:%MZ) --https-only \
  --auth-mode login --as-user --full-uri
```

BREAK IT

Allow public blob access on the account, set the container to `--public-access blob`, and fetch the file with plain `curl`. Count how many switches it took. Then turn both off.

PROOF FOR YOUR REPO

curl output while public and after you closed it. The expired SAS failing the next day.

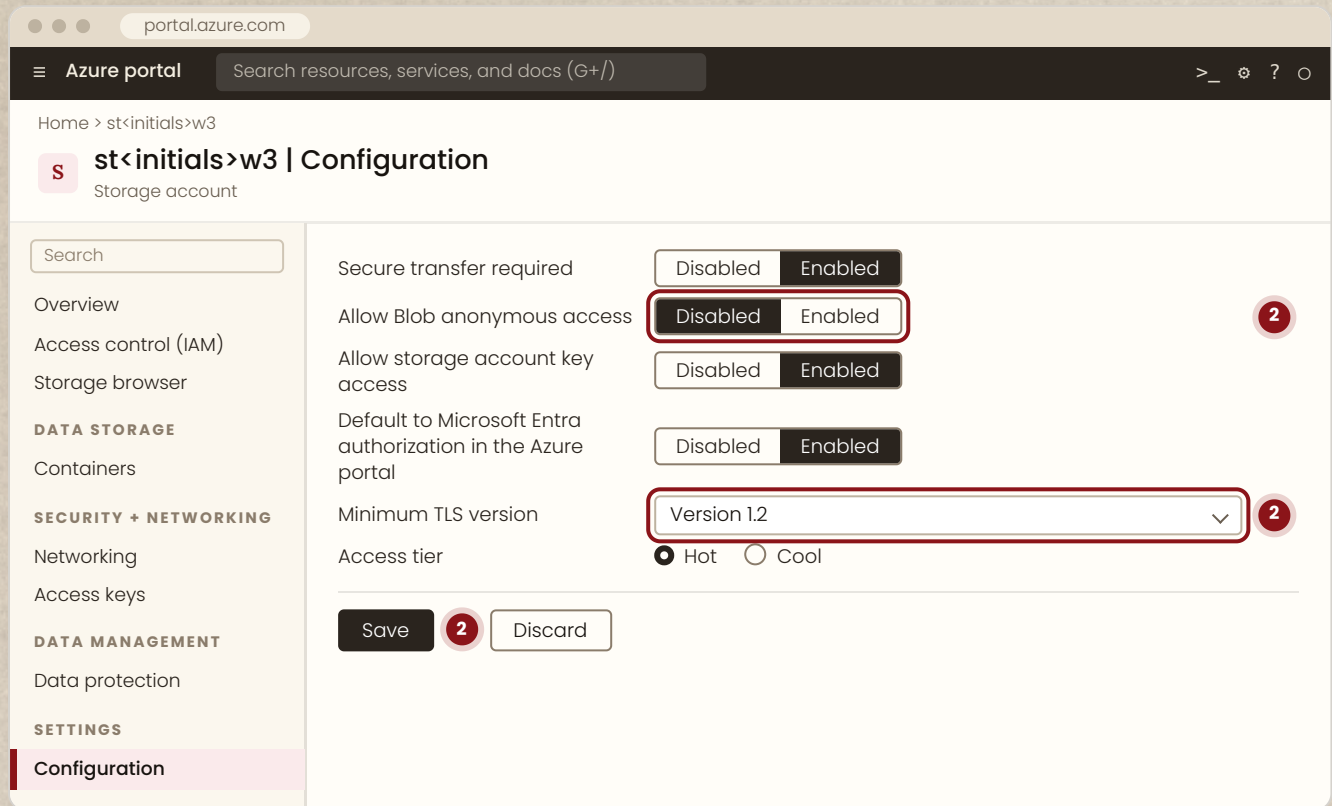
CLEAN UP

Keep everything for the week. Deallocate the VM each evening.

MENTOR QUESTION

Account key, account SAS, user delegation SAS: which would you give a partner, and why?

Four switches. All set to safe.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Create the storage account (Day 02 path) in rg-lab-w3, then open **Settings, Configuration**.
- 02** Allow Blob anonymous access **Disabled**, Minimum TLS version 1.2. Save.
- 03** Access control (IAM), Add role assignment: Storage Blob Data Contributor, to yourself.
- 04** Data storage, Containers, + Container: name `docs`, anonymous access level Private. Open it and Upload hello.txt.
- 05** Click hello.txt, **Generate SAS**: signing method User delegation key, Read only, expiry one hour ahead, HTTPS only. Generate and copy the Blob SAS URL.
- 06** Break it: anonymous access Enabled here, then docs, Change access level, Blob. curl it. Turn both off.

CHECK IT WORKED

Opening the plain blob URL in a private window fails. The SAS URL works until it expires.

12

75 min

Secrets belong in a vault. *Not in code.*

A password in a config file ends up in Git, in logs and in screenshots. Key Vault gives secrets one home with access control and history.

STEPS

- 01** Create a vault that uses Azure RBAC for access.

```
KV=kv-<initials>-$RANDOM
az keyvault create -n $KV -g rg-lab-w3 -l $LOC --enable-rbac-authorization true
KVID=$(az keyvault show -n $KV --query id -o tsv)
az role assignment create --assignee <your-upn> --role "Key Vault Secrets Officer" --scope $KVID
```

- 02** Store a generated secret, then rotate it and list versions.

```
az keyvault secret set --vault-name $KV -n db-password \
--value "$(openssl rand -base64 24)" -o none
# run the same command again to create version 2
az keyvault secret list-versions --vault-name $KV -n db-password -o table
```

- 03** Check the safety nets.

```
az keyvault show -n $KV --query "properties.
{softDelete:enableSoftDelete,purgeProtection:enablePurgeProtection}"
```

- 04** Notice the `-o none` above. Without it the secret value prints to your terminal and your shell history. Explain why that matters in a CI pipeline.

BREAK IT

Delete the secret, then get it back with `az keyvault secret recover`. Then try to purge it. What does purge protection change?

PROOF FOR YOUR REPO

Screenshot of the recovered secret versions. No secret values in the repo.

CLEAN UP

Keep the vault for Day 13.

MENTOR QUESTION

Why should an application never see a secret in its source code or pipeline logs, even a private repo?

Create the vault.

Decide recovery up front.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Key vaults >

Create a key vault

Basics Access configuration Networking Tags Review + create

Resource group * rg-lab-w3

Key vault name * kv-<initials>-01

Region South Africa North

Pricing tier Standard

Recovery options

Soft-delete Enabled (always on)

Days to retain deleted vaults 90

Purge protection ☒ Disable purge protection ☐ Enable purge protection

Review + create < Previous Next: Access configuration >

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Search "Key vaults", + Create.
- 02** Basics: rg-lab-w3, a unique name, your region, Standard.
- 03** Purge protection: Disable for this lab so you can see purge work. In the capstone you will enable it.
- 04** Access configuration tab: permission model **Azure role-based access control**. Review + create.
- 05** Vault, Access control (IAM): give yourself Key Vault Secrets Officer. Until you do, Secrets shows "not authorized".
- 06** Objects, Secrets, + Generate/Import: name db-password. Open it, then + New Version to rotate.
- 07** Delete the secret, then Manage deleted secrets, select it, Recover.

CHECK IT WORKED

db-password shows two versions, and survives one delete and recover.

13

90 min

Managed identity. *No keys at all.*

The best credential is one nobody can leak because nobody ever sees it. Let the VM prove who it is.

STEPS

- 01** Give the VM an identity and grant it read access to the blob and the secret.

```
PID=$(az vm identity assign -g rg-lab-w3 -n vm-web --query systemAssignedIdentity -o tsv)
az role assignment create --assignee-object-id $PID --assignee-principal-type ServicePrincipal \
  --role "Storage Blob Data Reader" --scope $SAID
az role assignment create --assignee-object-id $PID --assignee-principal-type ServicePrincipal \
  --role "Key Vault Secrets User" --scope $KVID
```

- 02** On the VM, write `day13/read.sh` and run it through `run-command`. It asks the metadata service for a token, then reads the blob.

```
TOKEN=$(curl -s -H Metadata:true \
  "http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://storage.azure.com/" \
  | python3 -c "import sys,json;print(json.load(sys.stdin)['access_token'])")
curl -s -H "Authorization: Bearer $TOKEN" -H "x-ms-version: 2020-04-08" \
  https://<sa>.blob.core.windows.net/docs/hello.txt
```

- 03** Switch off account keys completely. Confirm the VM still works.

```
az storage account update -n $SA -g rg-lab-w3 --allow-shared-key-access false
```

- 04** Extend the script to read the db-password secret from Key Vault with a token for `https://vault.azure.net`.

BREAK IT

The metadata endpoint answers any process on the VM. If a web app on this VM had an SSRF bug, what could an attacker take? Why does Azure require the `Metadata: true` header?

PROOF FOR YOUR REPO

`read.sh` in the repo. Never paste a full token into notes or screenshots.

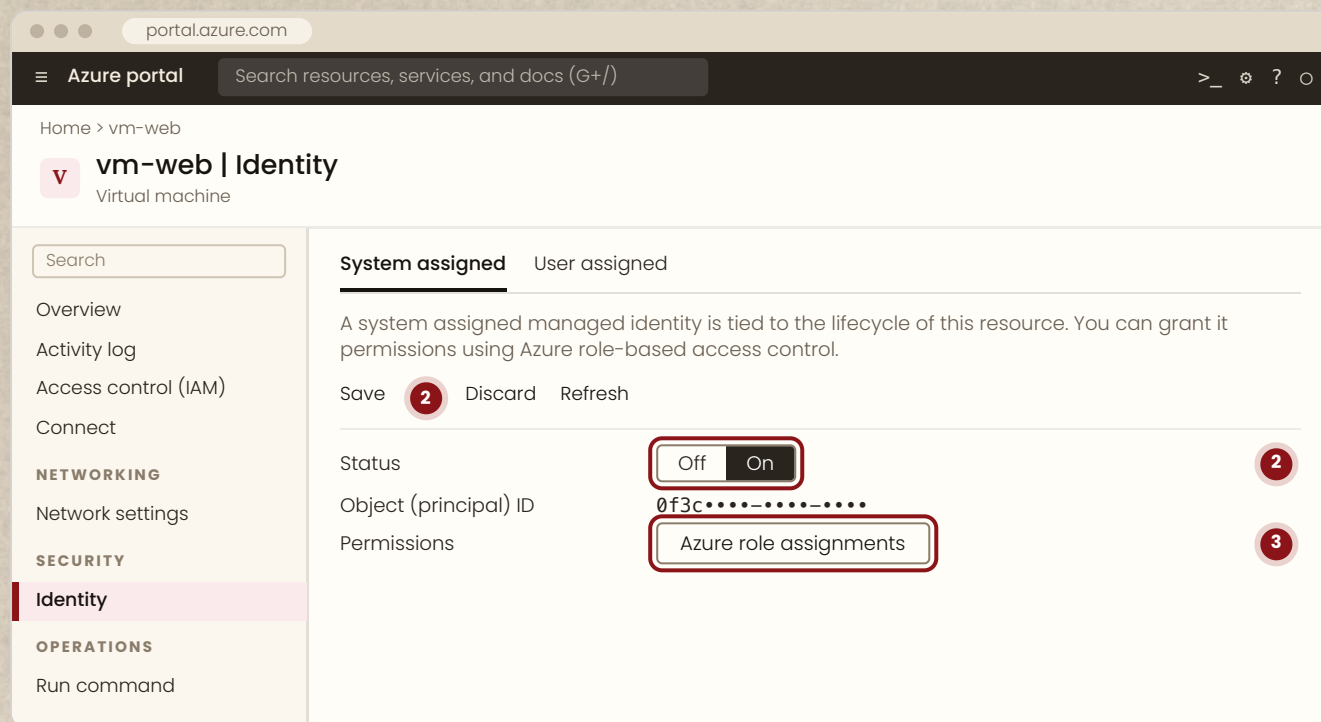
CLEAN UP

Keep everything for Day 14.

MENTOR QUESTION

System assigned or user assigned identity: when would you choose each?

Turn the identity on. Then give it one job.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Open **vm-web**. Under Security choose **Identity**.
- 02** **System assigned** tab: Status On, Save, confirm Yes.
- 03** **Azure role assignments**, + **Add role assignment**: scope Storage, your account, role Storage Blob Data Reader. Save.
- 04** **Add another**: scope Key Vault, your vault, role Key Vault Secrets User.
- 05** **Storage account, Configuration**: Allow storage account key access Disabled. Save.
- 06** Run **read.sh** through Run command (Day 08 path).
- 07** **Storage account, Access keys**: note what the page says now that keys are off.

CHECK IT WORKED

Run command prints hello, while every request signed with an account key fails.

14

90 min

Private endpoints. Off the internet.

Even with perfect RBAC, a storage account on a public endpoint can be reached from anywhere. Move it inside your network.

STEPS

01 Create the private endpoint in snet-data.

```
az network private-endpoint create -g rg-lab-w3 -n pe-blob --vnet-name vnet-lab \
  --subnet snet-data --private-connection-resource-id $SAID \
  --group-id blob --connection-name blob-conn
```

02 Wire up private DNS, so the normal name resolves to the private IP inside the VNet.

```
Z=privatelink.blob.core.windows.net
az network private-dns zone create -g rg-lab-w3 -n $Z
az network private-dns link vnet create -g rg-lab-w3 -z $Z -n link-lab \
  --virtual-network vnet-lab --registration-enabled false
az network private-endpoint dns-zone-group create -g rg-lab-w3 --endpoint-name pe-blob \
  -n default --private-dns-zone $Z --zone-name blob
```

03 Close the public door.

```
az storage account update -n $SA -g rg-lab-w3 --public-network-access Disabled
```

04 Compare `nslookup <sa>.blob.core.windows.net` from the VM and from your laptop. Run `read.sh` on the VM, then try to list blobs from your laptop.**BREAK IT**

Delete the DNS zone group. What does `nslookup` return on the VM now, and does `read.sh` still work? Put it back afterwards.

PROOF FOR YOUR REPO

Both `nslookup` outputs side by side, with one line explaining the difference.

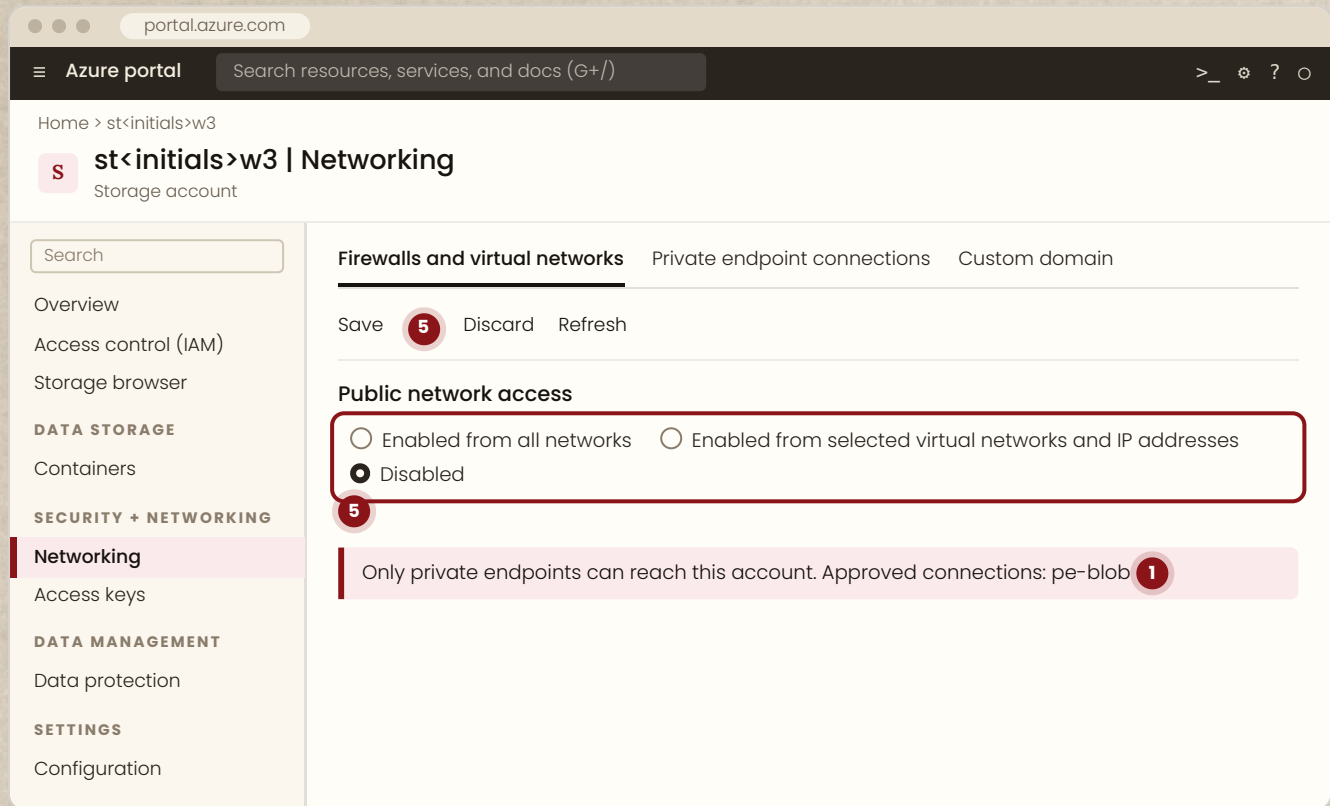
CLEAN UP

Private endpoints bill by the hour. Delete them at the end of the week with the resource group.

MENTOR QUESTION

Service endpoint or private endpoint: what is the real difference, and when is each enough?

Add the private door. Then close the public one.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Storage account, Networking, Private endpoint connections, + Private endpoint.
- 02 Basics: rg-lab-w3, **pe-blob**, your region. **Resource**: sub-resource blob.
- 03 Virtual Network tab: vnet-lab, snet-data.
- 04 DNS tab: Integrate with private DNS zone **Yes**. Review + create.
- 05 Back on Networking: Public network access **Disabled**. Save.
- 06 Open Storage browser from your laptop: an access error, because you are outside the VNet. That is the point.
- 07 Private DNS zones: open the privatelink.blob zone and find your A record.

CHECK IT WORKED

Private endpoint connections lists **pe-blob** as **Approved**, and the A record points to a 10.10.3.x address.

15

75 min

Plan for mistakes. Then recover from one.

Security includes getting things back. Deletion, overwrites and ransomware all test the same controls.

STEPS

- 01 Turn on soft delete and versioning.** Run data commands from the VM, or temporarily allow your IP on the storage firewall.

```
az storage account blob-service-properties update --account-name $SA -g rg-lab-w3 \
  --enable-delete-retention true --delete-retention-days 7 --enable-versioning true
```

- 02 Overwrite** hello.txt with new content, then list versions with `az storage blob list --include v`. Restore the old version.

- 03 Delete the blob**, then bring it back with `az storage blob undelete`.

- 04 Lock the resource group** and try to delete the storage account.

```
az lock create -n no-delete -g rg-lab-w3 --lock-type CanNotDelete
```

- 05 Snapshot the VM disk.**

```
DISK=$(az vm show -g rg-lab-w3 -n vm-web --query storageProfile.osDisk.managedDisk.id -o tsv)
az snapshot create -g rg-lab-w3 -n snap-web --source $DISK
```

BREAK IT

Give labreader Contributor on rg-lab-w3. As labreader, try to remove the lock. Which permission is missing? Remove the role afterwards.

PROOF FOR YOUR REPO

Version list before and after the restore. Plus your Week 3 write up.

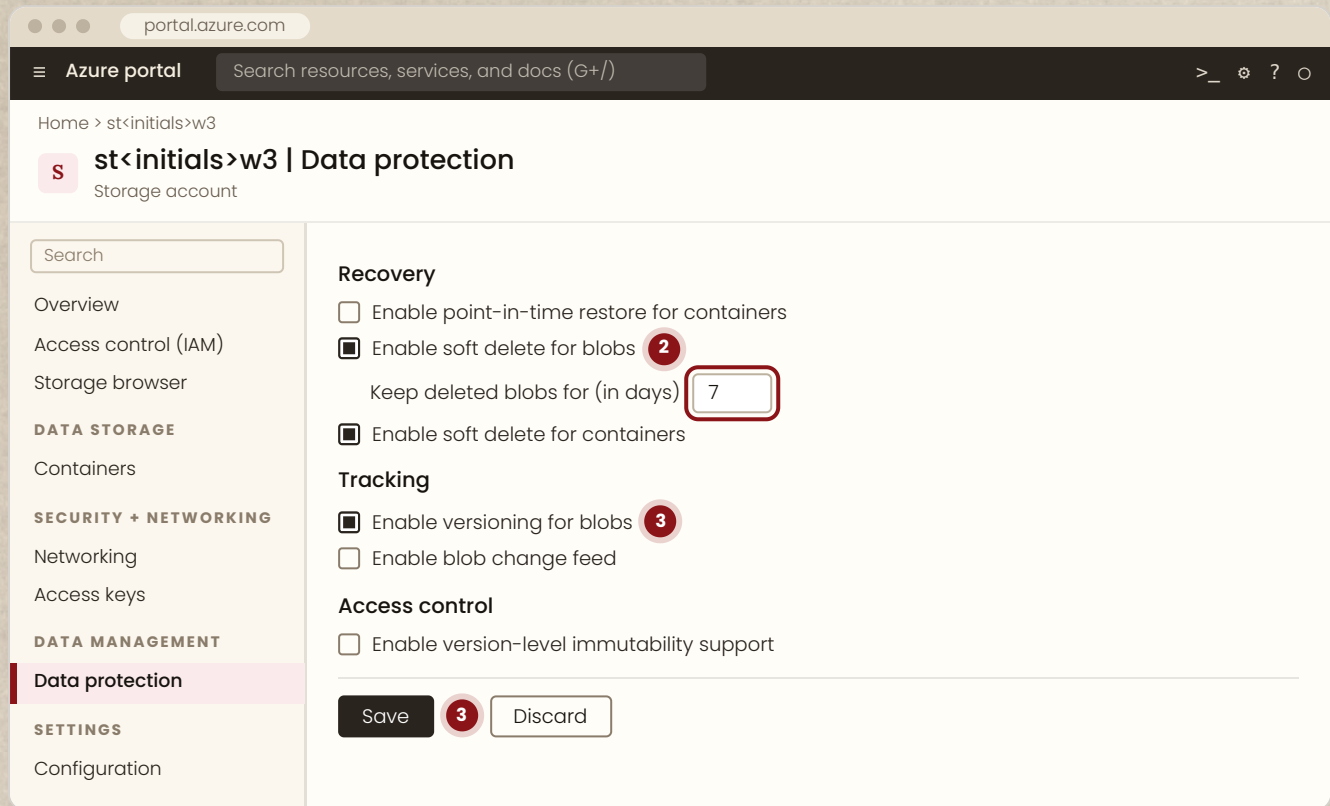
CLEAN UP

Remove the lock, then `az group delete -n rg-lab-w3 --yes --no-wait`.

MENTOR QUESTION

Ransomware deletes backups first. Which of today's controls would slow an attacker down, and which would not?

Tick the safety nets. Before you need them.



Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01** Storage account, Data management, Data protection. If data pages fail, allow your client IP under Networking for today.
- 02** Tick soft delete for blobs, 7 days.
- 03** Tick versioning for blobs. Save.
- 04** Containers, docs, hello.txt, Versions tab: select the older version, Make current version.
- 05** Delete hello.txt. Turn on Show deleted blobs, select it, Undelete.
- 06** rg-lab-w3, Settings, Locks, + Add: name no-delete, lock type Delete. Try deleting the storage account.
- 07** Search "Disks", open vm-web's OS disk, + Create snapshot.

CHECK IT WORKED

The delete is blocked by the lock, and hello.txt is back with its version history.

16

90 min

Turn on the logs. Then ask them questions.

You cannot investigate what you never recorded. Send logs to one place and learn enough KQL to answer simple questions.

STEPS

01 Create a workspace and a storage account to watch.

```
az group create -n rg-lab-w4 -l $LOC --tags owner=<yourname> purpose=lab
az monitor log-analytics workspace create -g rg-lab-w4 -n law-lab
LAWID=$(az monitor log-analytics workspace show -g rg-lab-w4 -n law-lab --query id -o tsv)
```

02 Export the Activity Log: Monitor, then Activity log, then Export Activity Logs. Send Administrative, Security and Policy to law-lab.

03 Send blob access logs to the workspace as well.

```
az monitor diagnostic-settings create -n to-law --workspace $LAWID \
--resource $SAID/blobServices/default \
--logs '[{"category":"StorageRead","enabled":true}, {"category":"StorageWrite","enabled":true}, {"category":"StorageDelete","enabled":true}]'
```

04 Ask questions in KQL under Logs in the workspace.

```
AzureActivity
| where TimeGenerated > ago(1d)
| summarize count() by OperationNameValue, Caller
| top 20 by count_

StorageBlobLogs
| project TimeGenerated, OperationName, CallerIpAddress, AuthenticationType, Uri
```

BREAK IT

Do five things: create, tag and delete a resource, read a blob, fail a read. Find every one in the logs. How long did each take to appear?

PROOF FOR YOUR REPO

Your queries saved as `day16/*.kql`, with one line on what each answers.

CLEAN UP

Keep rg-lab-w4 for the rest of the month.

MENTOR QUESTION

Which log shows who read a blob: the Activity Log or the resource logs? Why are they separate?

Pick the categories.

Pick where they go.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Monitor | Activity log >

M Diagnostic setting

Diagnostic setting name *

Logs: Categories

- ☒ Administrative
- ☒ Security
- ☐ ServiceHealth
- ☐ Alert
- ☐ Recommendation
- ☒ Policy
- ☐ Autoscale
- ☐ ResourceHealth

Destination details

- ☒ Send to Log Analytics workspace
 -
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

Save Discard Delete

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Search "Log Analytics workspaces", + Create: rg-lab-w4, law-lab.
- 02 Search "Monitor", Activity log, Export Activity Logs, then + Add diagnostic setting.
- 03 Name it to-law.
- 04 Tick Administrative, Security and Policy.
- 05 Send to Log Analytics workspace: law-lab. Save.
- 06 Storage account, Monitoring, Diagnostic settings, blob, + Add diagnostic setting: StorageRead, StorageWrite, StorageDelete to law-lab.
- 07 law-lab, Logs: switch to KQL mode, paste the lab queries, Run.

CHECK IT WORKED

AzureActivity returns rows within about 15 minutes, and StorageBlobLogs shows your reads.

17

90 min

Read the scorecard. *Fix what matters.*

Defender for Cloud's free tier scores your posture against the Microsoft cloud security benchmark. The skill is choosing what to fix first.

STEPS

01 Open Defender for Cloud. The foundational posture features are free. Do not enable paid plans such as Servers or Storage.

02 Note your secure score, then open Recommendations and sort by severity.

03 Pull the list with Resource Graph so you can track it.

```
az graph query -q "securityresources
| where type == 'microsoft.security/assessments'
| where properties.status.code == 'Unhealthy'
| project rec=tostring(properties.displayName),
sev=tostring(properties.metadata.severity),
res=tostring(properties.resourceDetails.Id)"
```

04 Fix five recommendations in your lab resources. For each, write the risk in one sentence before you fix it.

05 Open Regulatory compliance and find which benchmark controls your fixes moved.

BREAK IT

Pick one recommendation you will not fix. Exempt it with a written reason and an expiry date. Real teams make this call every week.

PROOF FOR YOUR REPO

Before and after secure score, the five risk sentences, and the exemption reason.

CLEAN UP

Keep everything.

MENTOR QUESTION

Your secure score went up ten percent. Is the company ten percent safer? Argue both sides.

Read the list.

Choose what goes first.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud

D Microsoft Defender for Cloud | Recommendations

Search

GENERAL

- Overview
- Getting started
- Recommendations**
- Attack path analysis
- Security alerts
- Inventory

CLOUD SECURITY

- Security posture
- Regulatory compliance
- Workload protections

MANAGEMENT

- Environment settings

Secure score **58%**

Active recommendations **14**

Download CSV report **7** Open query Group by

Recommendation (examples)	Severity	Affected
Management ports should be closed on your virtual machines	High	1 of 1
Storage accounts should restrict network access	Medium	1 of 2
Key vaults should have deletion protection enabled	Medium	1 of 1
Machines should have vulnerability findings resolved	High	1 of 1

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Search "Microsoft Defender for Cloud".** Overview shows your secure score.
- 02 Recommendations.** Sort by severity. Some tenants show risk level instead.
- 03 Open one recommendation.** Read Description, Remediation steps and Affected resources. Some have a Fix button.
- 04 Environment settings, your subscription, Defender plans:** look, and leave the paid plans Off.
- 05 Exempt one:** in a recommendation, Exempt, category Mitigated or Waiver, an expiry date and your reason.
- 06 Regulatory compliance:** open the Microsoft cloud security benchmark and find the controls your fixes moved.
- 07 Download CSV report** before and after, for your repo.

CHECK IT WORKED

Five recommendations move to Healthy within a day, and one shows as Exempt with your reason.

18

120 min

Set the alarms. Then trip them.

An alert nobody receives is a log entry. Wire alerts to you, then cause and investigate an incident.

STEPS

- 01 Create an action group** that emails you.

```
az monitor action-group create -g rg-lab-w4 -n ag-lab --short-name lab --action email me <your-email>
```

- 02 Alert on three risky operations.** Repeat with `Microsoft.Network/networkSecurityGroups/securityRules/write` and `Microsoft.Storage/storageAccounts/listKeys/action`.

```
az monitor activity-log alert create -g rg-lab-w4 -n al-role-assign \
  --scope /subscriptions/$SUB --action-group ag-lab \
  --condition category=Administrative and \
  operationName=Microsoft.Authorization/roleAssignments/write
```

- 03 Stage it.** Give labreader Contributor on rg-lab-w4. As labreader, list storage keys and add an NSG rule opening 22 to anywhere.

- 04 Investigate.** Build the timeline from the logs.

```
AzureActivity
| where Caller =~ "labreader@<domain>"
| project TimeGenerated, OperationNameValue, ActivityStatusValue, CallerIpAddress, ResourceGroup
| order by TimeGenerated asc
```

- 05 Contain.** Remove the role, delete the rule, `az storage account keys renew`.

BREAK IT

Write a one page incident report: timeline, what was touched, how you knew, containment, and what you would change.

PROOF FOR YOUR REPO

`day18/incident-report.md` and the alert emails as screenshots.

CLEAN UP

Delete labreader. Keep rg-lab-w4 for the capstone.

MENTOR QUESTION

Which alert arrived first, how many minutes after the action, and would anyone have seen it at 3am?

Choose the signal. Choose who hears it.

portal.azure.com

Azure portal Search resources, services, and docs (G+)

Home > Monitor | Alerts >

M Create an alert rule

Scope **Condition** Actions Details Tags Review + create

Signal name * Create role assignment (Role Assignment) 3

Signal type Activity Log

Alert logic

Event level All selected

Status All selected

Event initiated by * (All services and users)

Preview

Whenever the Activity Log has an event with Category='Administrative', Signal name='Create role assignment'

Review + create Previous Next: Actions > 4

Illustration, simplified. Numbers match the click path. The live portal changes often, so labels may move.

CLICK PATH

- 01 Monitor, Alerts, Action groups, + Create:** rg-lab-w4, name ag-lab. Notifications: Email, your address. Create.
- 02 Monitor, Alerts, + Create, Alert rule.** Scope: your subscription.
- 03 Condition:** See all signals, search role assignment, choose **Create role assignment**.
- 04 Actions:** Select action groups, ag-lab.
- 05 Details:** rg-lab-w4, name al-role-assign. Review + create.
- 06 Repeat** for Create or Update Security Rule and for List Storage Account Keys.
- 07 After the staged incident:** Monitor, Alerts shows what fired. Open one to see the event, then build the timeline in law-lab, Logs.

CHECK IT WORKED

Three alert rules are Enabled, and each one fires an email during the staged incident.

19 20

Build it once. Build it secure. From code.

Everything from the month in one Bicep deployment. It must deploy with one command, show no changes on a second what-if run, and tear down with one command.

REQUIREMENTS

- **Governance.** One resource group with owner, purpose and expires tags. Allowed locations and required tag policies.
- **Network.** VNet with web, app and data subnets. An NSG on each. No 22 or 3389 open to the internet.
- **Compute.** One Linux VM, no public IP, system assigned identity, nginx installed through cloud-init.
- **Storage.** No public blob access, no shared keys, TLS 1.2, private endpoint, soft delete and versioning.
- **Secrets.** Key Vault with RBAC and purge protection. Only the VM identity can read the secret.
- **Visibility.** Log Analytics, diagnostic logs for storage and Key Vault, an alert on role assignments.

DELIVERABLES

A `capstone/` folder with the Bicep, and a README holding: an architecture diagram, five risks with the control that answers each, deploy and destroy commands, and a cost estimate.

DAY 20: THE REVIEW

A 15 minute walkthrough with your mentor. Deploy live, open Defender for the resource group, show the logs, then answer "why" for any control your mentor points at.

SCORED ON

Works deploys clean. **Secure** meets every requirement. **Explained** each control justified. **Clean** teardown leaves nothing billing.

DONE MEANS

Someone who has never seen Azure could clone the repo, deploy it, understand why it is safe, and delete it.

Twenty days. Twenty proofs.

Fill in the date and the repo link as each lab finishes. The mentor ticks the last box after reading the proof and the answer to the mentor question.

DAY	LAB	DONE ON	PROOF LINK	MENTOR
01	Set up like a professional			☐
02	One resource, three ways			☐
03	Entra ID users and groups			☐
04	RBAC and scope			☐
05	Azure Policy guardrails			☐
06	Plan and build a VNet			☐
07	First VM, the safe way			☐
08	Lose the public IP			☐
09	Peering and traffic tests			☐
10	Hunt the exposure			☐
11	Storage done right			☐
12	Key Vault			☐
13	Managed identity			☐
14	Private endpoints			☐
15	Recovery and locks			☐
16	Logs and KQL			☐
17	Defender for Cloud			☐
18	Alerts and a mini incident			☐
19	Capstone build			☐
20	Capstone review			☐

EVERY EVENING, TWO MINUTES

Deallocate VMs. Glance at Cost analysis. Commit your notes. Unfinished labs roll to the weekend, never past it.