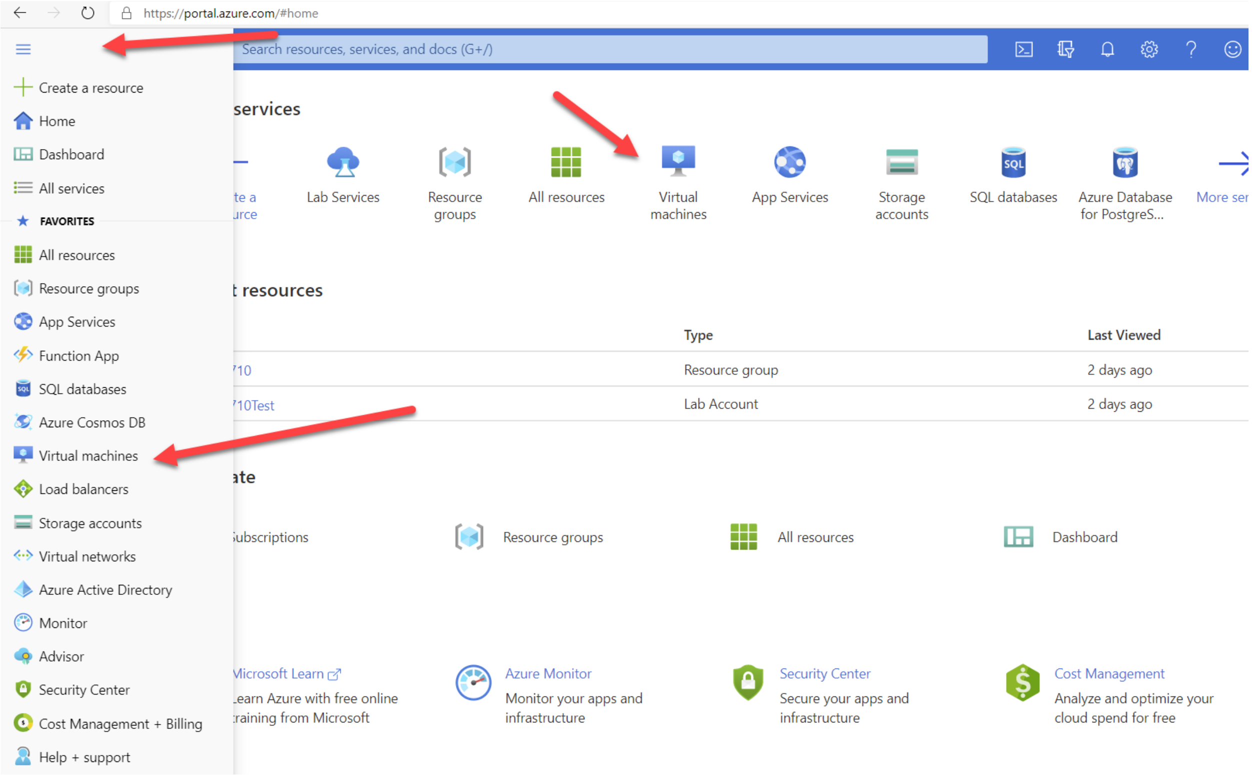
Lab:
Creating Virtual Machines (VM) in Azure

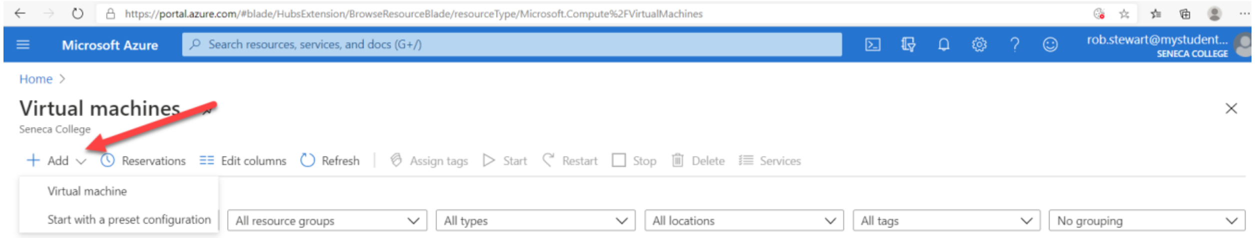
Pre-Work:

- You will need Remote Desktop (RDP). It should be pre-installed with Windows 10 machines – just type remote desktop in the search bar
- Or you can download a specific version here Microsoft RDP

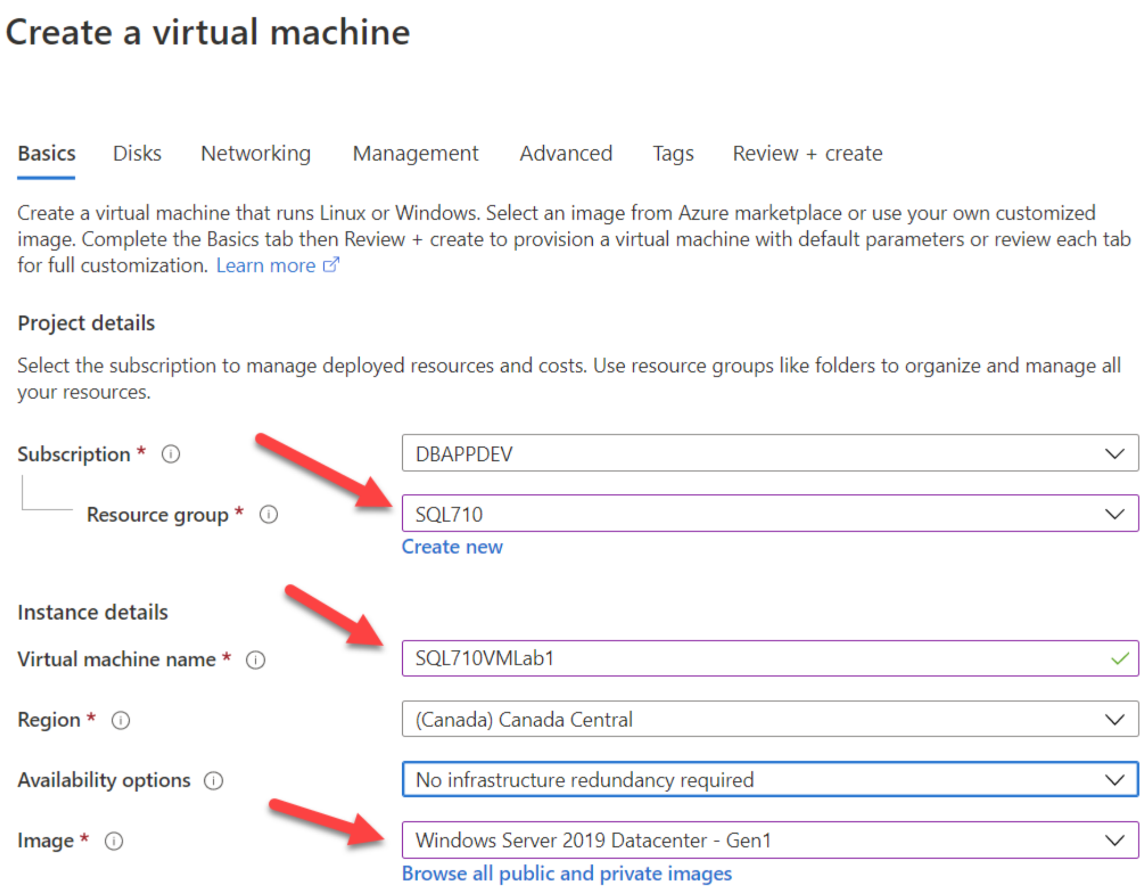
1. Login into Azure https://portal.azure.com using your school scredentials.
2. Select Virtual Machines from either the icon from the Azure Services or click the “Hamburger Menu Button” ≡ at the top left of the screen and then select the Virtual Machines menu option.



3. Select ADD



4. Select Virtual Machine to create a new VM



Create a virtual machine

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 * : DBAPPDEV

Resource group * : SQL710

Create new

Instance details

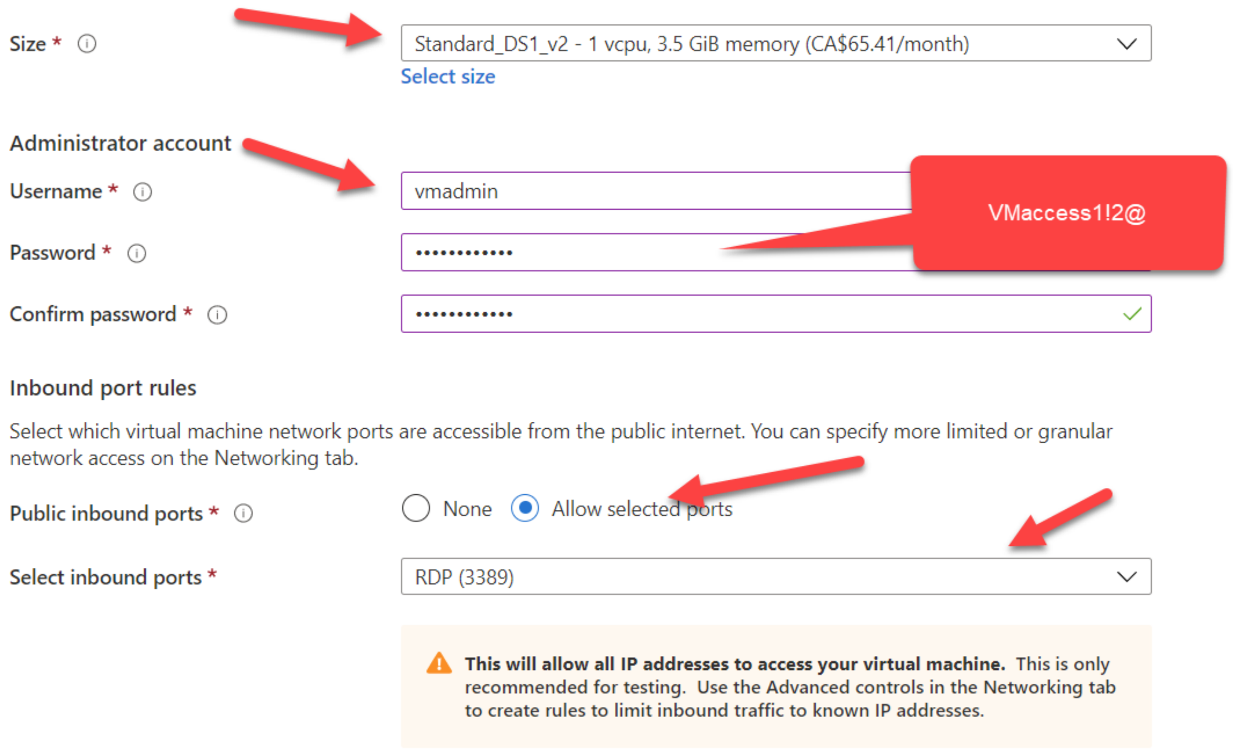
Virtual machine name * : SQL710VMLab1 ✓

Region * : (Canada) Canada Central

Availability options : No infrastructure redundancy required

Image * : Windows Server 2019 Datacenter - Gen1

Browse all public and private images



Size * ⓘ
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (CA$65.41/month)
Select size

Administrator account

Username * ⓘ vmadmin

Password * ⓘ ••••••••••••

Confirm password * ⓘ •••••••••••• ✓

VMaccess1!2@

Inbound port rules

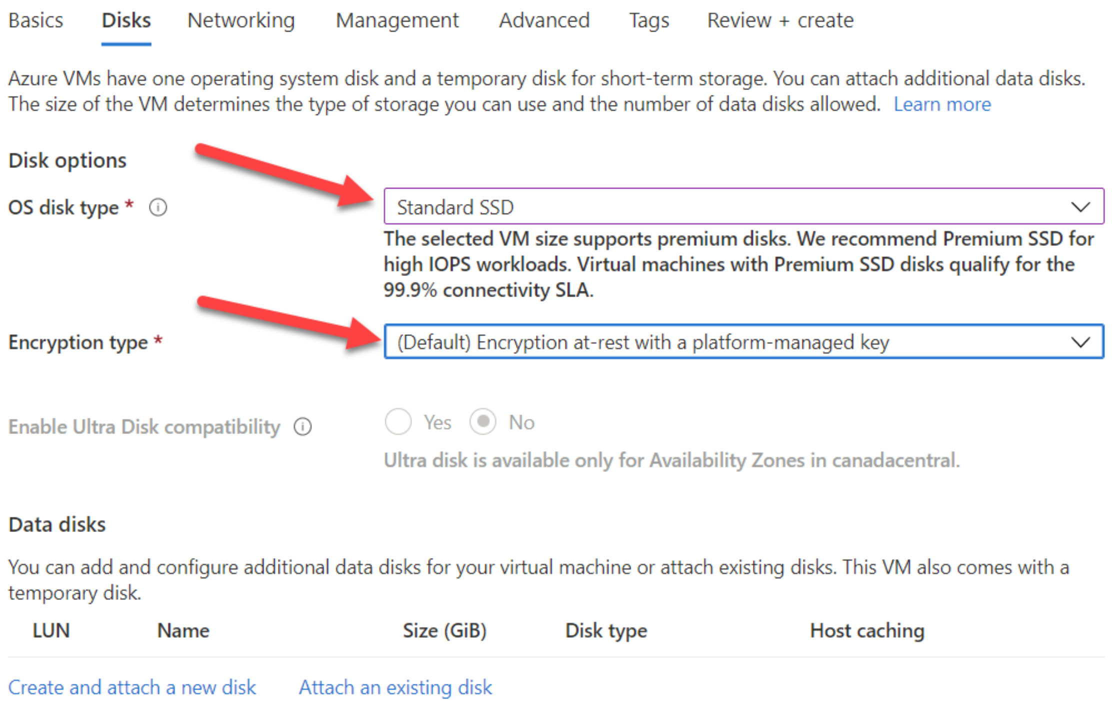
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ○ None ● Allow selected ports

Select inbound ports * RDP (3389)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

5. Set licensing to NO.
6. Click on **Next: Disks>**



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

Disk options

OS disk type * ⓘ Standard SSD

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.

Encryption type * (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ ○ Yes ● No

Ultra disk is available only for Availability Zones in canadacentral.

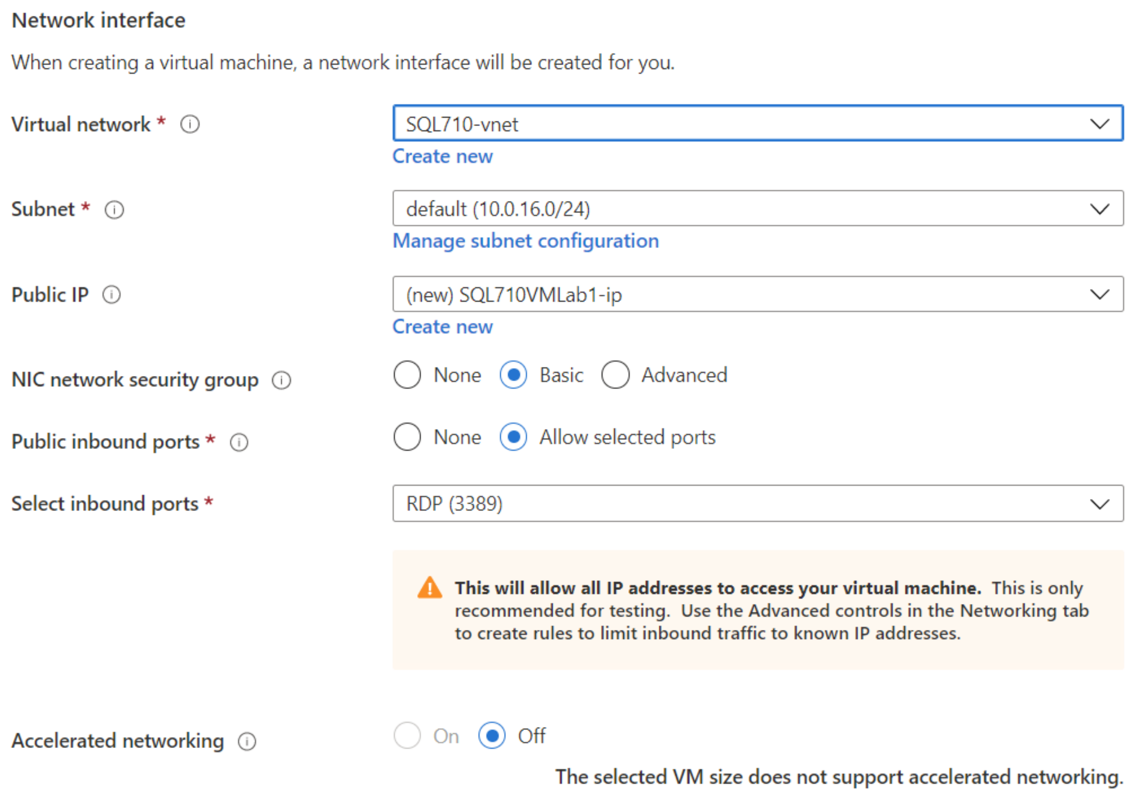
Data disks

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

Create and attach a new disk   Attach an existing disk

7. Click on **Next: Networking>**



Network interface

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

Virtual network * ⓘ SQL710-vnet

Subnet * ⓘ default (10.0.16.0/24)

Public IP ⓘ (new) SQL710VMLab1-ip

NIC network security group ⓘ ○ None ● Basic ○ Advanced

Public inbound ports * ⓘ ○ None ● Allow selected ports

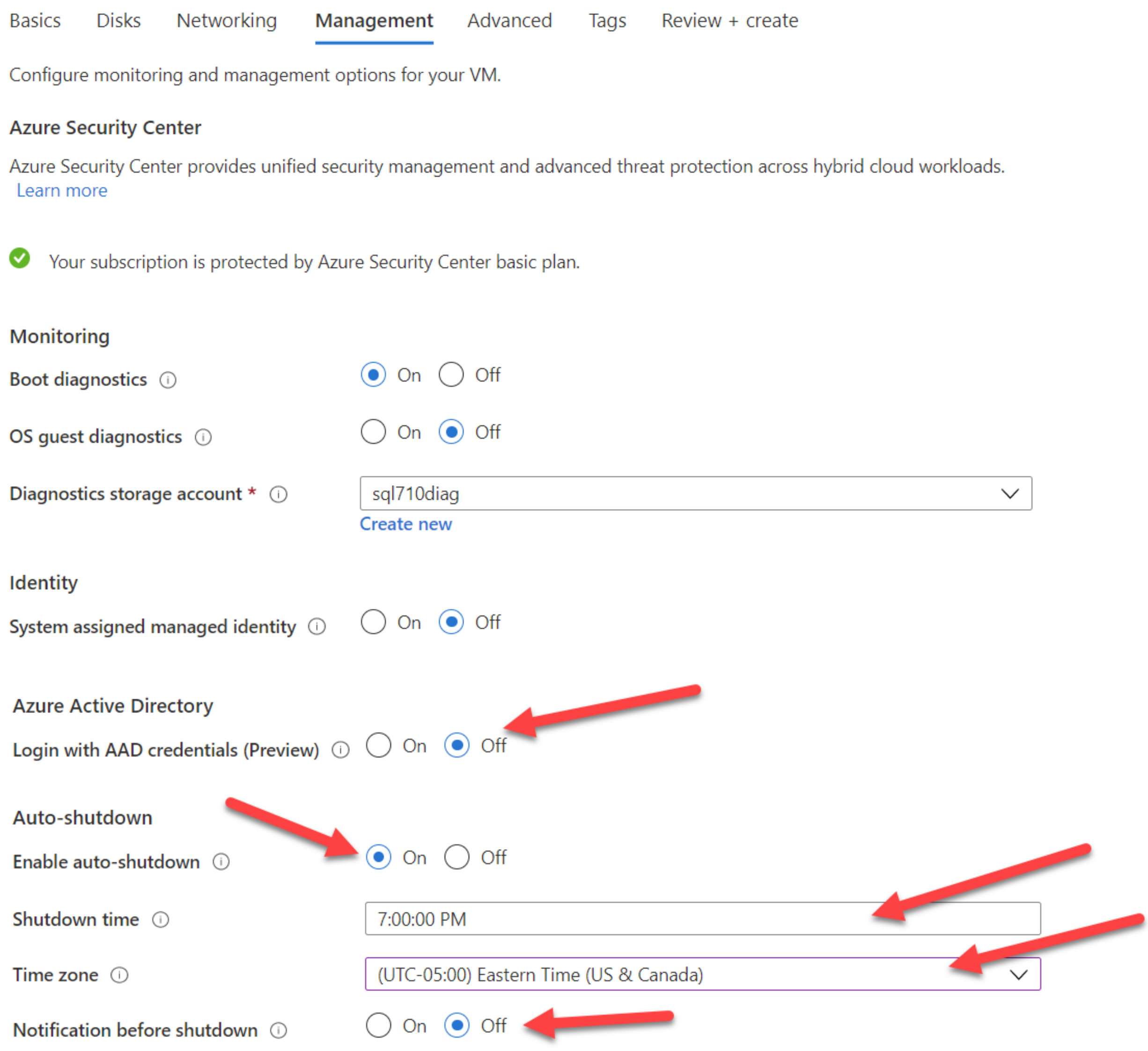
Select inbound ports * RDP (3389)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking ⓘ ○ On ● Off

The selected VM size does not support accelerated networking.

8. Select NO for load balancing solution
9. Click on **Next: Management>**



Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ ● On ○ Off

OS guest diagnostics ⓘ ○ On ● Off

Diagnostics storage account * ⓘ sql710diag
Create new

Identity

System assigned managed identity ⓘ ○ On ● Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ ○ On ● Off

Auto-shutdown

Enable auto-shutdown ⓘ ● On ○ Off

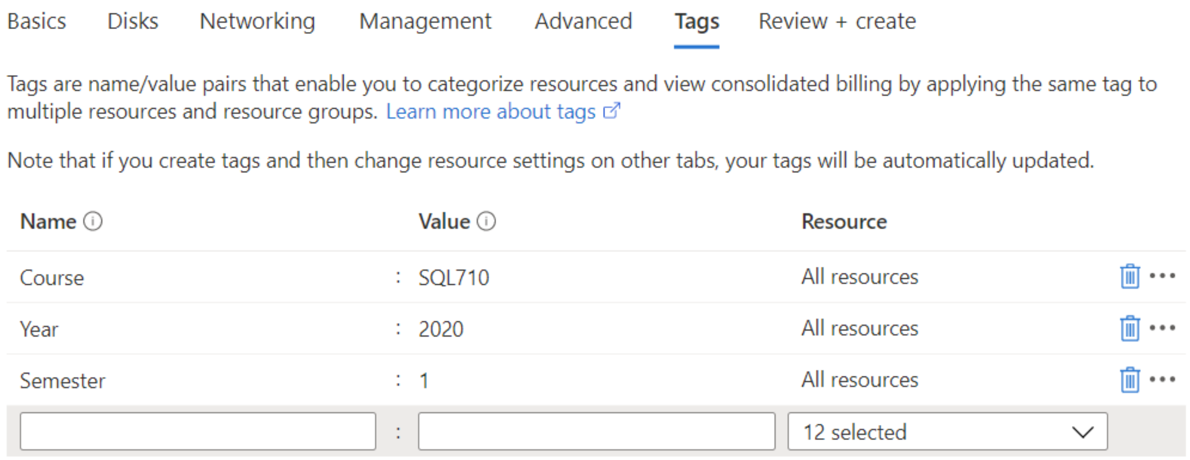
Shutdown time ⓘ 7:00:00 PM

Time zone ⓘ (UTC-05:00) Eastern Time (US & Canada)

Notification before shutdown ⓘ ○ On ● Off

10. **Click Next: Advanced>**
11. Leave Advanced settings as is.

12. Click **Next: Tags>**



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

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name		Value	Resource
Course	:	SQL710	All resources
Year	:	2020	All resources
Semester	:	1	All resources
	:		12 selected

13. Click **Next: Review + create>**
14. Click **Create**
15. Click **Go to Resource**
16. Select CONNECT from the side menu
17. Click on **Download RDP File**
18. Open downloaded RDP file and it should automatically start RDP and you will be prompted for the user name and password (vmadmin:VMaccess1!2@)

Note: That this configuration has port 3389 (RDP) open to all IP addresses and is not secure other than the username/password

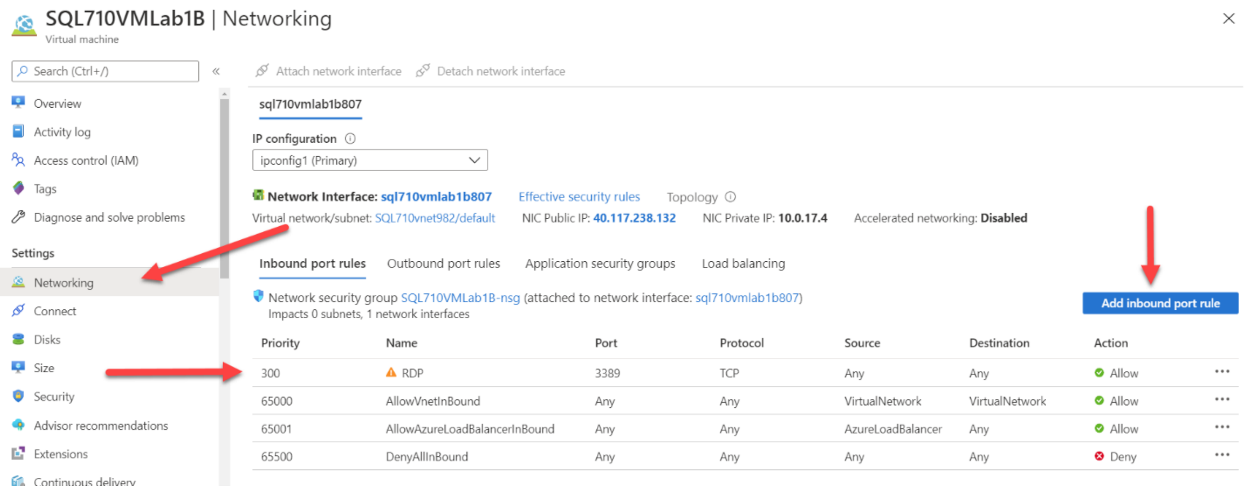
What we would like to do is lock down the RDP port access to specific IP addresses.
Follow the steps below to lock down the RDP access across the public IP network.

1. Find your public IP(v4) address of your local machine (You do NOT want your private IP):

   In a browser search engine type
   Whats my IP

   Or just go here https://www.whatsmyip.org/

2. Select the NETWORKING tab in Azure VM



IP configuration: ipconfig1 (Primary)

Network Interface: sql710vmlab1b807

Virtual network/subnet: SQL710vnet982/default NIC Public IP: 40.117.238.132 NIC Private IP: 10.0.17.4 Accelerated networking: Disabled

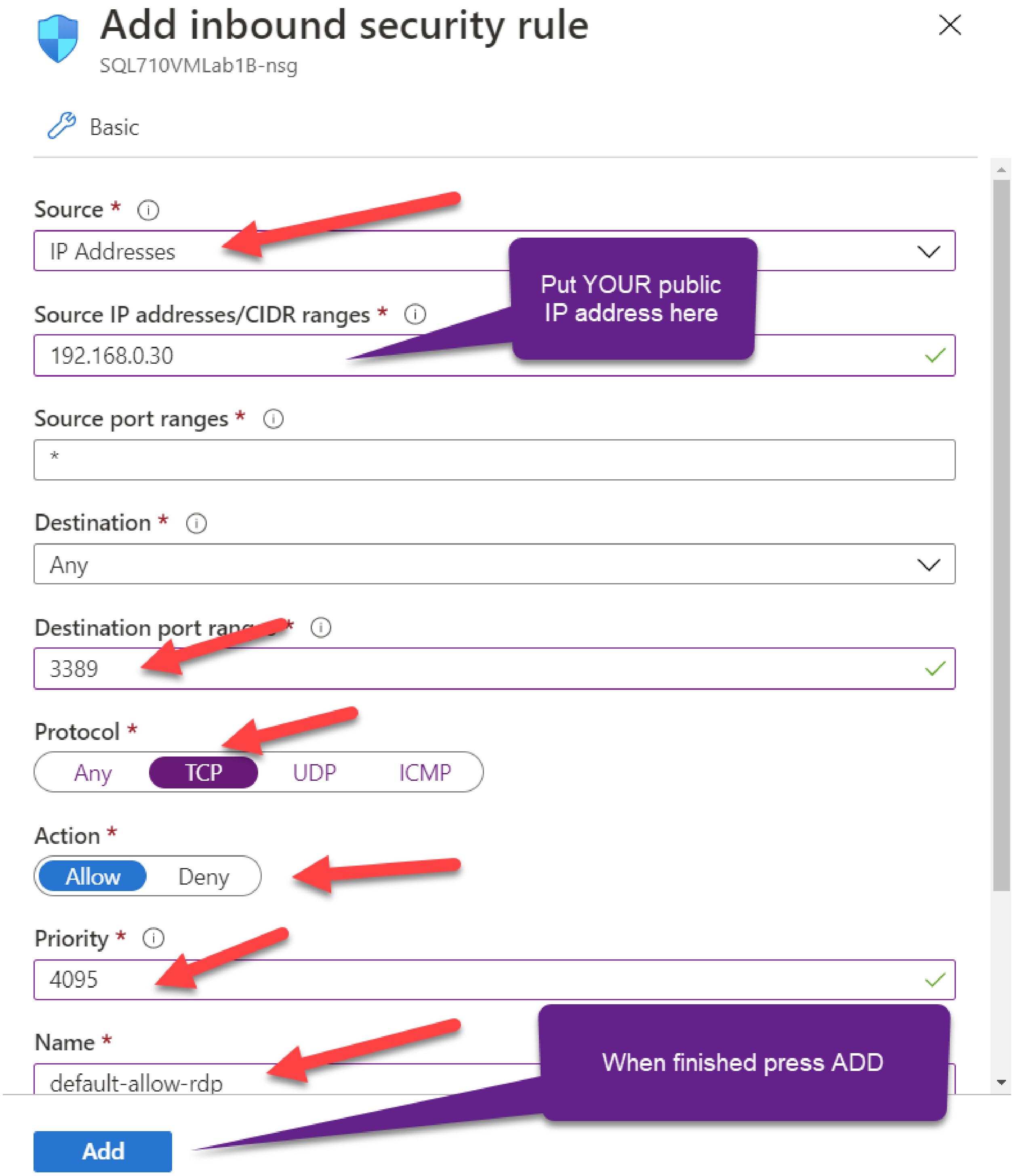
Network security group SQL710VMLab1B-nsg (attached to network interface: sql710vmlab1b807)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
300	⚠ RDP	3389	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

Note: That the Inbound Security Rule allows ALL IP sources access to the RDP port. We want to lock that down to specific IP sources for added security.

3. Click on the RDP Inbound Security Rule
4. Delete this security rule

5. Create a new RDP Inbound Security Rule
6. Click on **Add Inbound port rule**



Add inbound security rule

SQL710VMLab1B-nsg

Basic

Source * : IP Addresses

Source IP addresses/CIDR ranges * : 192.168.0.30

Source port ranges * : *

Destination * : Any

Destination port ranges * : 3389

Protocol * : Any [✓ TCP] UDP ICMP

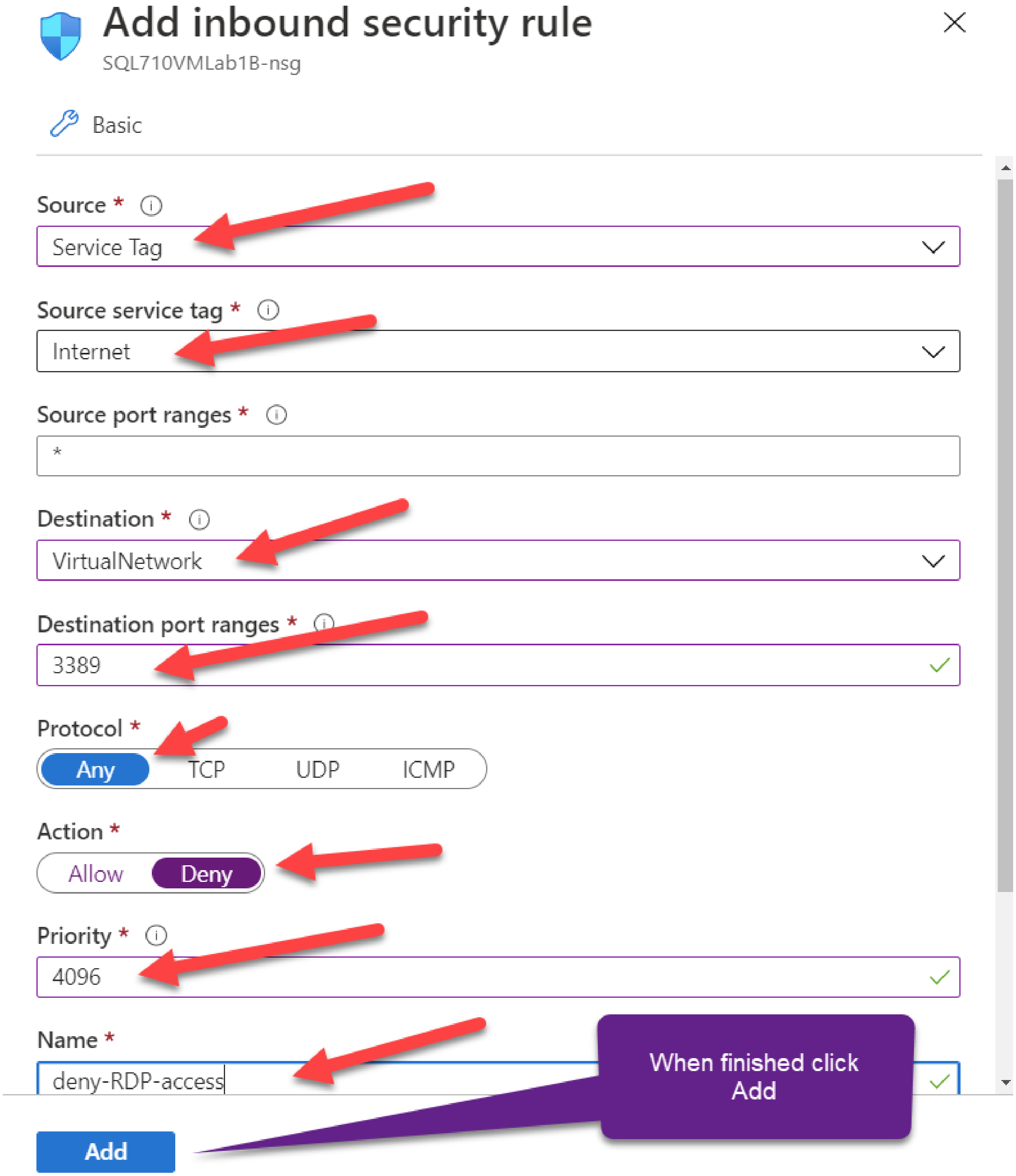
Action * : [✓ Allow] Deny

Priority * : 4095

Name * : default-allow-rdp

7. Now we will block all protocols from all IP addresses from accessing port 3389 on our Virtual Network

8. Create another inbound port rule. Click on **Add inbound port rule**



Add inbound security rule

SQL710VMLab1B-nsg

Basic

Source * : Service Tag

Source service tag * : Internet

Source port ranges * : *

Destination * : VirtualNetwork

Destination port ranges * : 3389

Protocol * : [✓ Any] TCP UDP ICMP

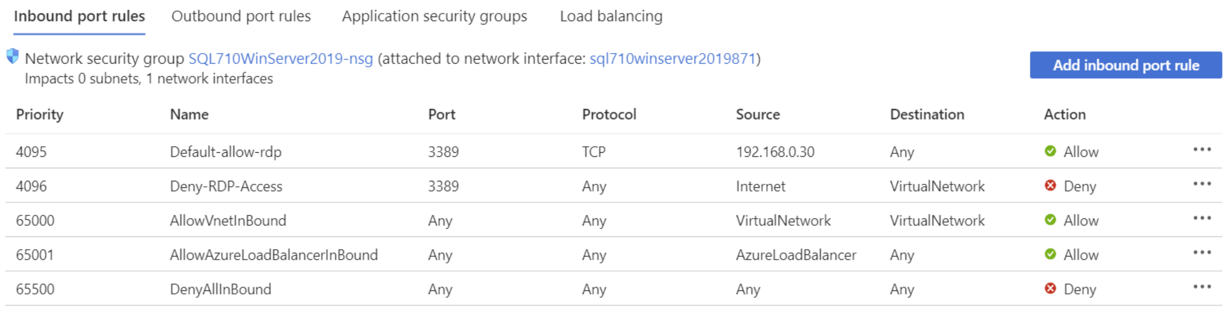
Action * : Allow [✓ Deny]

Priority * : 4096

Name * : deny-RDP-access

When finished click Add

Note: You will now see the 2 new inbound security port rules you created



Network security group SQL710WinServer2019-nsg (attached to network interface: sql710winserver2019871)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
4095	Default-allow-rdp	3389	TCP	192.168.0.30	Any	✓ Allow
4096	Deny-RDP-Access	3389	Any	Internet	VirtualNetwork	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

What we have done is

- Allowed RDP from a specific IP address or range
- Deny all other RDP traffic

Note: Rules are checked in the order of priority. Once a rule applies, no more rules are tested for matching.

Note: You can improve on this type of security by enabling "Just-in-time access" from Azure. Just-in-time access enables you to lock down inbound traffic to your VM by allowing access for only a limited time. JIT access requires an updated subscription (ie: more money)