

# AZ-104 Administer Virtual Networking



# Learning Objectives - Administer Virtual Networking

- Configure Virtual Networks
- Configure Network Security Groups
- Host your domain on Azure DNS
- Lab 04 – Implement Virtual Networks

# Configure Virtual Networks



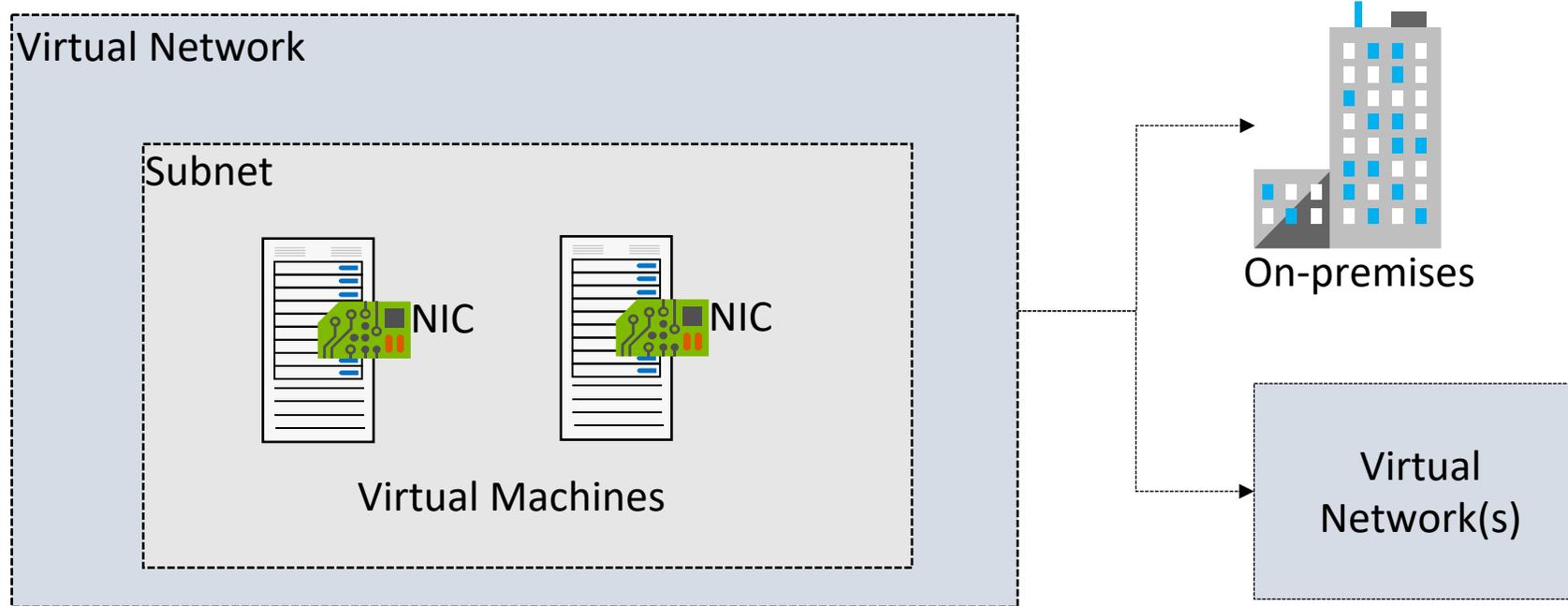
# Learning Objectives - Configure Virtual Networks

- Plan Virtual Networks
- Create Virtual Networks
- Create Subnets
- Plan IP Addressing
- Create Public IP Addresses
- Associate Public IP Addresses
- Allocate or Assign Private IP Addresses
- Demonstration – Virtual Networks
- Learning Recap

Implement and manage virtual networking (15–20%): Configure and manage virtual networks in Azure

- Create and configure virtual networks and subnets
- Configure public IP addresses

# Plan Virtual Networks



Logical representation  
of your own network

Create a dedicated  
private cloud-only  
virtual network

Securely extend  
your datacenter with  
virtual networks

Enable hybrid  
cloud scenarios

# Create Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Define the address space, and at least one subnet
- Check for overlapping address spaces

## Create virtual network

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

### Project details

Subscription \* ⓘ Visual Studio Enterprise ▾

Resource group \* ⓘ Lab04 ▾

[Create new](#)

### Instance details

Name \* VNet2 ✓

Region \* (US) East US 2 ▾

# Create Subnets

+ Subnet + Gateway subnet Refresh | Manage users Delete

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/26	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

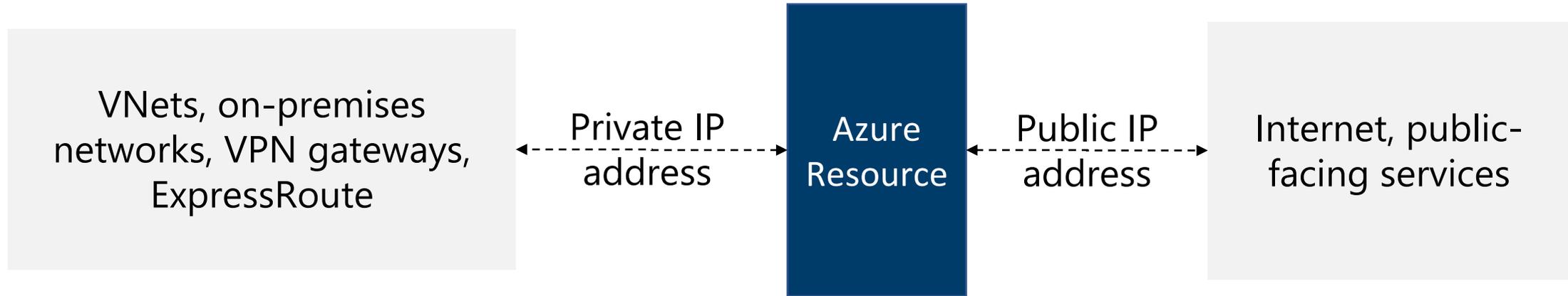
A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription

# Plan IP Addressing



**Private IP addresses** - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

**Public IP addresses** - used for communication with the Internet, including Azure public-facing services

# Create Public IP Addresses

IPv4 or IPv6

Standard SKU – do you need to upgrade?

Regional vs Global

Microsoft network vs. Internet

The screenshot shows the 'Create public IP address' configuration page in the Azure portal. The page has a title bar with 'Create public IP address' and a three-dot menu icon. Below the title bar are four tabs: 'Basics' (selected), 'DDoS Protection', 'Tags', and 'Review + create'. The main content area is titled 'Configuration details' and contains several configuration options:

- Name \***: A text input field.
- IP Version \* ⓘ**: Radio buttons for 'IPv4' (selected) and 'IPv6'.
- SKU \* ⓘ**: Radio buttons for 'Standard' (selected) and 'Premium'.
- Availability zone \* ⓘ**: A dropdown menu showing 'Zone-redundant'.
- Tier \* ⓘ**: Radio buttons for 'Regional' (selected) and 'Global'.
- IP address assignment**: A text input field.
- IP address assignment \* ⓘ**: Radio buttons for 'Dynamic' and 'Static' (selected).
- Routing preference \* ⓘ**: Radio buttons for 'Microsoft network' (selected) and 'Internet'.

# Associate Public IP Addresses

<b>Top-level resource</b>	<b>IP address configuration</b>
Virtual Machine	Network interface
Virtual Network Gateway (VPN), Virtual Network Gateway (ER), NAT Gateway	Gateway IP configuration
Public Load Balancer, Application Gateway, Azure Firewall, Route Server, API Management	Front-end configuration
Bastion Host	Public IP configuration

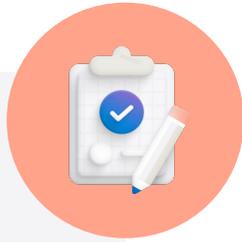
# Allocate or Assign Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

**Dynamic (default).** Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

**Static.** You select and assign any unassigned or unreserved IP address in the subnet's address range

# Learning Recap – Virtual Networks



Check your  
knowledge  
questions and  
additional  
study

## Reference modules

- [Introduction to Azure Virtual Networks](#)
- [Design an IP addressing schema for your Azure deployment](#)
- [Implement Windows Server IaaS VM IP addressing and routing](#)

# Configure Network Security Groups (NSGs)



# Learning Objectives – Network Security Groups

- Implement Network Security Groups
- Determine NSG Rules
- Determine NSG Effective Rules
- Create NSG Rules
- Implement Application Security Groups
- Demonstration – NSGs
- Learning Recap

Implement and manage virtual networking (15–20%): Configure secure access to virtual networks

- Create and configure network security groups (NSGs) and application security groups
- Evaluate effective security rules in NSGs

# Implement Network Security Groups

The screenshot displays the Azure portal interface for a Network Security Group (nsg0). The top left shows the shield icon and the name 'nsg0' with the subtitle 'Network security group'. To the right, it indicates the directory as 'Microsoft'. Below this is a search bar with the placeholder 'Search (Ctrl+)' and a double arrow icon. A navigation menu on the left lists: Overview (selected), Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area features action buttons: Move, Delete, and Refresh. The configuration details are as follows:

Resource group ( <a href="#">change</a> )	: rg01	Custom security rules	: 1 inbound, 0 outbound
Location	: East US	Associated with	: 1 subnets, 0 network interfaces
Subscription ( <a href="#">change</a> )	:		
Subscription ID	:		
Tags ( <a href="#">change</a> )	: <a href="#">Click here to add tags</a>		

Limits network traffic to resources in a virtual network

Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

# Determine NSG Rules

## Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	 RDP_Inbound	3389	Any	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny

## Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

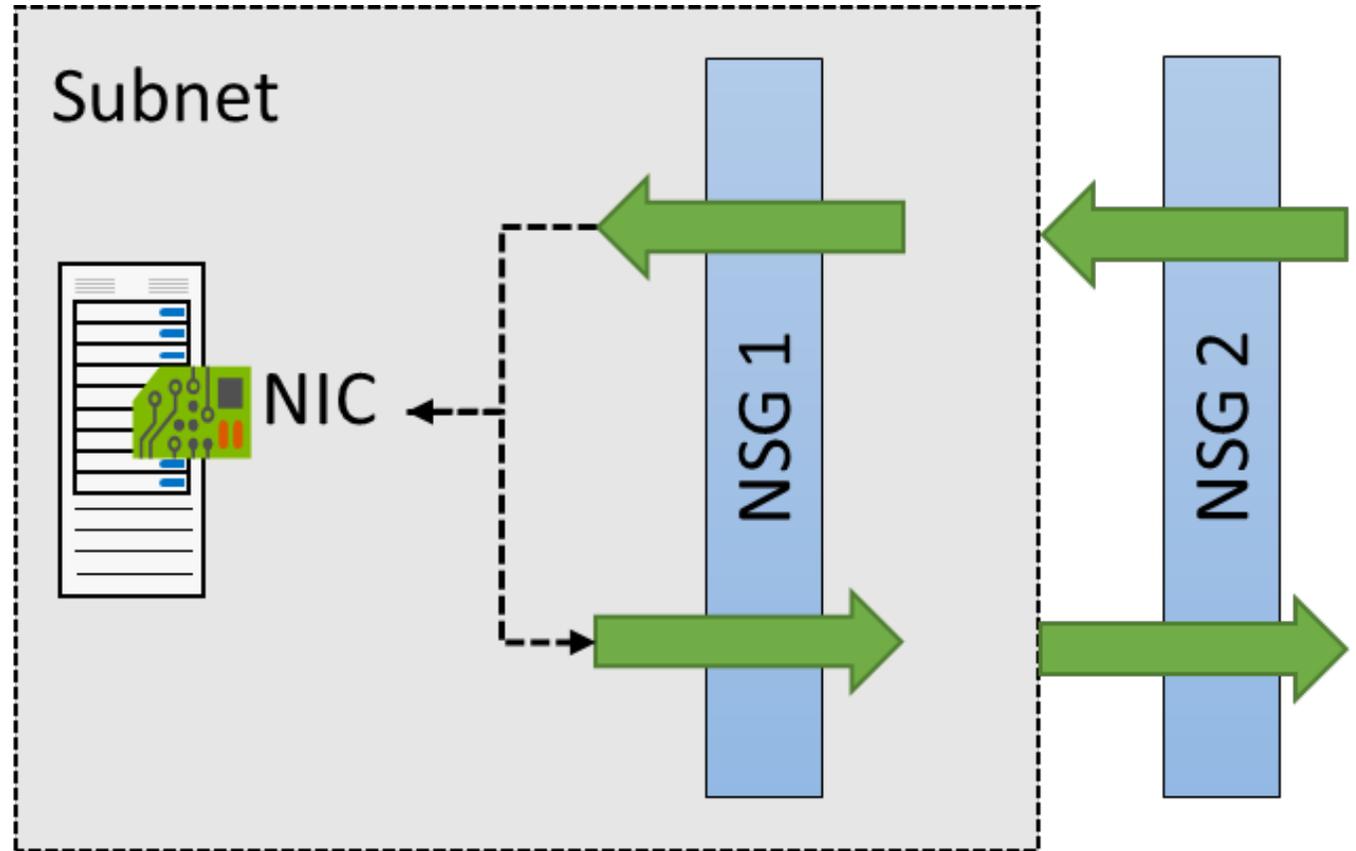
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

# Determine NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An "allow" rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



 Network Interface: **vm01990**

[Effective security rules](#)

[Topology](#)

Virtual network/subnet: [vnet01/subnet0](#)

NIC Public IP: -

NIC Private IP: **10.1.0.4**

Accelerated networking: **Disabled**

# Create NSG rules

**Source** (Any, IP addresses, My IP address, service tags, and application security group)

**Destination** (Any, IP addresses, service tag, and application security group)

**Service** (HTTPS, SSH, RDP, DNS, POP3, custom, ...)

**Priority** – The lower the number, the higher the priority

**Add inbound security rule**  
nsgtest

Source ⓘ  
Any

Source port ranges \* ⓘ  
\*

Destination ⓘ  
Any

Service ⓘ  
Custom

Destination port ranges \* ⓘ  
8080

Protocol  
 Any  UDP  
 TCP  ICMPv4

Action  
 Allow  Deny

Priority \* ⓘ  
100

Name \*  
AllowAnyCustom8080Inbound

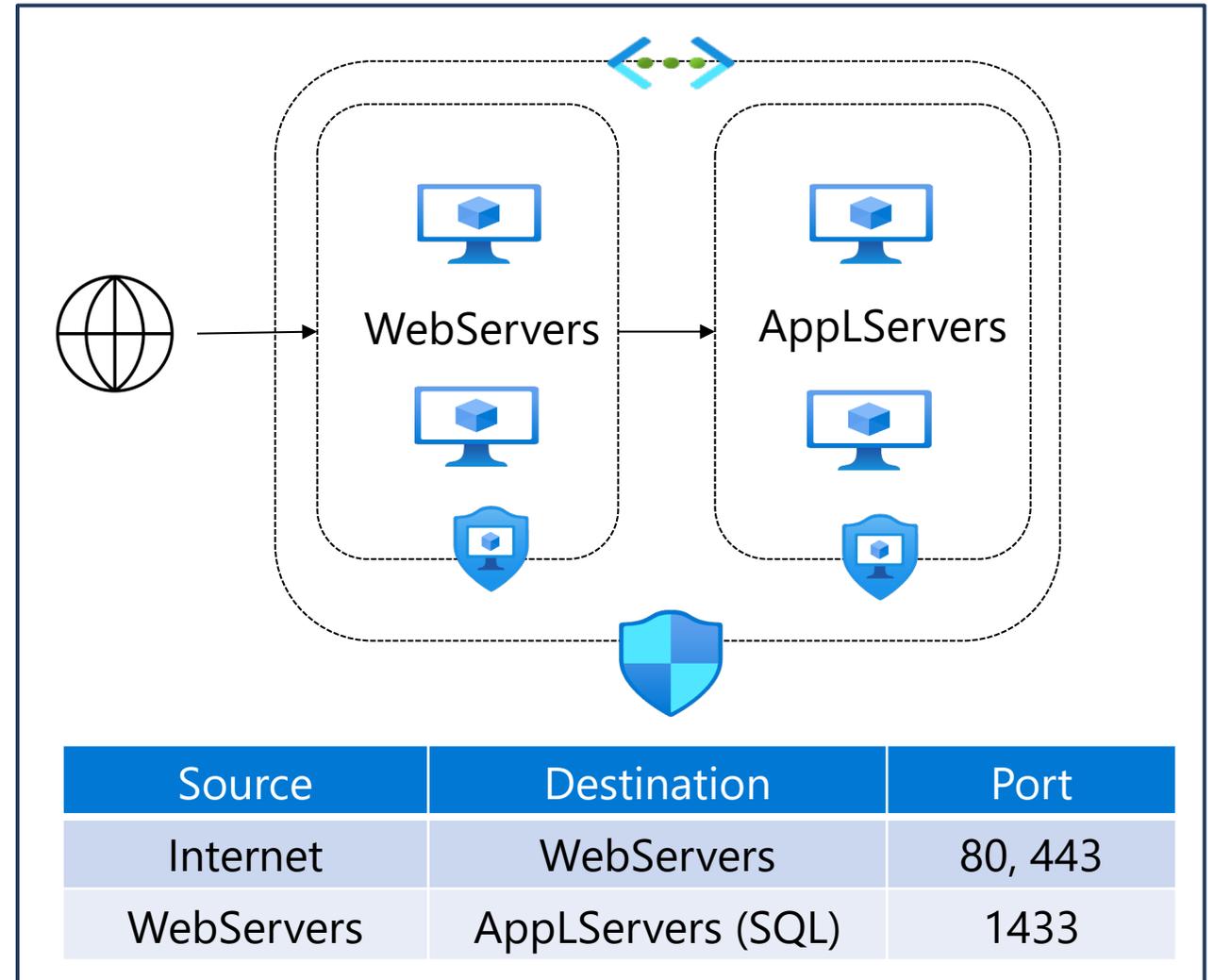
# Implement Application Security Groups

Extends your application's structure

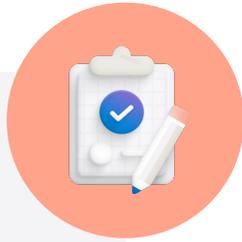
ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



# Learning Recap – Network Security Groups



Check your  
knowledge  
questions and  
additional  
study

## Reference modules

- [Configure network security groups](#)
- [Filter network traffic with a network security group using the Azure portal](#)
- [Secure and isolate access to Azure resources by using network security groups and service endpoints](#)

# Host your domain on Azure DNS



# Learning Objectives - Host your domain on Azure DNS

- What is Azure DNS?
- Configure Azure DNS to host your domain
- Verify delegation of domain name services
- Dynamically resolve resource name by using alias record
- Configure a private DNS zone
- Demonstration – DNS Name Resolution
- Learning Recap

Implement and manage virtual networking (15–20%): Configure name resolution and load balancing

- Configure Azure DNS

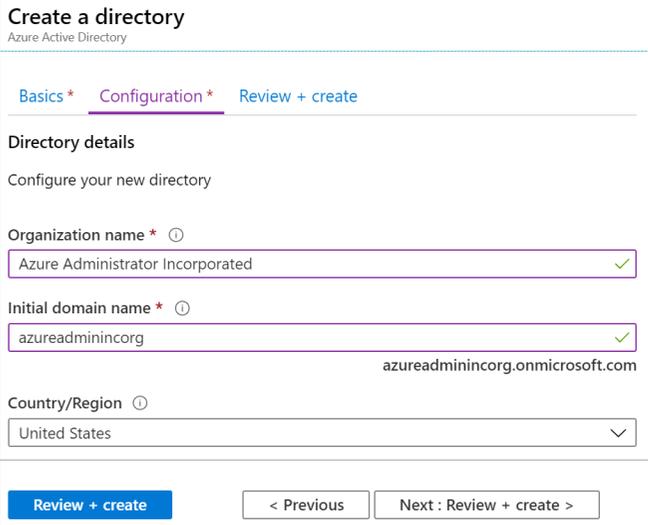
# What is Azure DNS?

When you create a new tenant, a new default domain is created

The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can add a custom domain name

After the custom name is added it must be verified – this demonstrates ownership of the domain



**Create a directory**  
Azure Active Directory

[Basics \\*](#) [Configuration \\*](#) [Review + create](#)

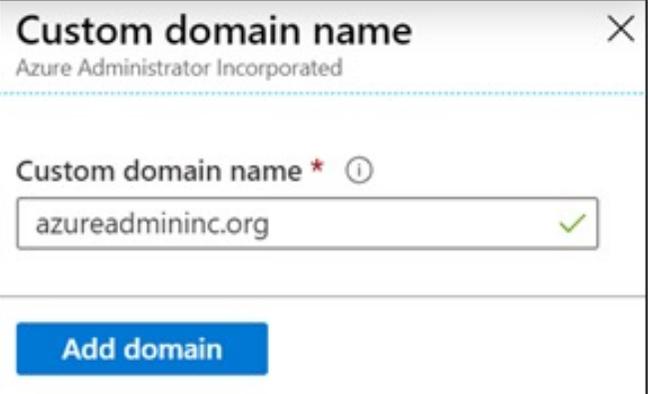
**Directory details**  
Configure your new directory

Organization name \* ⓘ  
Azure Administrator Incorporated ✓

Initial domain name \* ⓘ  
azureadminincorg ✓  
azureadminincorg.onmicrosoft.com

Country/Region ⓘ  
United States ▼

[Review + create](#) [< Previous](#) [Next : Review + create >](#)



**Custom domain name** ✕  
Azure Administrator Incorporated

Custom domain name \* ⓘ  
azureadmininc.org ✓

[Add domain](#)

# Configure Azure DNS to host your domain

A DNS zone hosts the DNS records for a domain

Where multiple zones share the same name, each instance is assigned different name server addresses

Root/Parent domain is registered at the registrar and pointed to Azure NS

## Create DNS zone



Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

### Project details

Subscription \*

Resource group \*  [Create new](#)

### Instance details

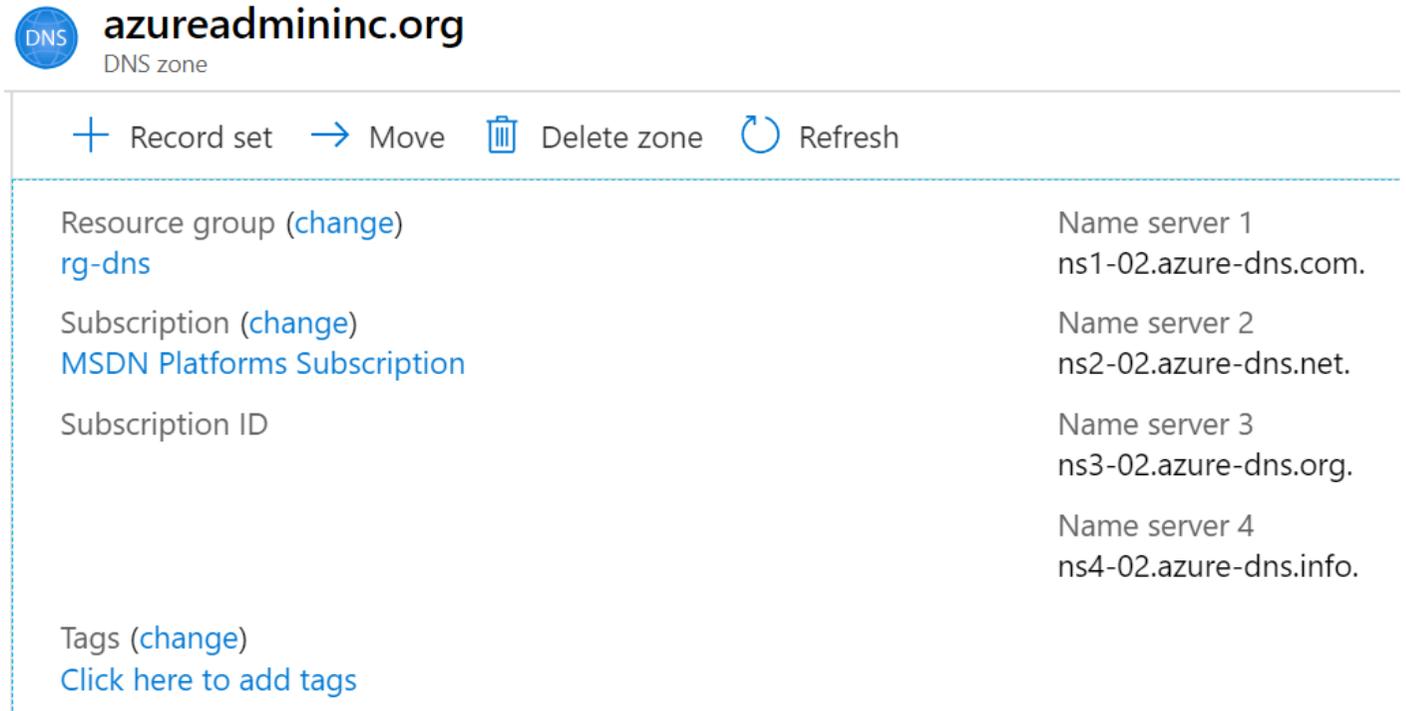
Name \*

Resource group location ⓘ

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

# Verify delegation of domain name services

- When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four
- Once the DNS zone is created, update the parent registrar
- For child zones, register the NS records in the parent domain



The screenshot displays the Azure portal interface for a DNS zone named 'azureadmininc.org'. At the top, there is a header with a 'DNS' icon, the domain name, and 'DNS zone'. Below the header is a toolbar with icons for '+ Record set', 'Move', 'Delete zone', and 'Refresh'. The main content area is divided into two columns. The left column contains metadata: 'Resource group (change) rg-dns', 'Subscription (change) MSDN Platforms Subscription', and 'Subscription ID'. The right column lists four name servers: 'Name server 1 ns1-02.azure-dns.com.', 'Name server 2 ns2-02.azure-dns.net.', 'Name server 3 ns3-02.azure-dns.org.', and 'Name server 4 ns4-02.azure-dns.info.'. At the bottom, there is a 'Tags (change) Click here to add tags' link.

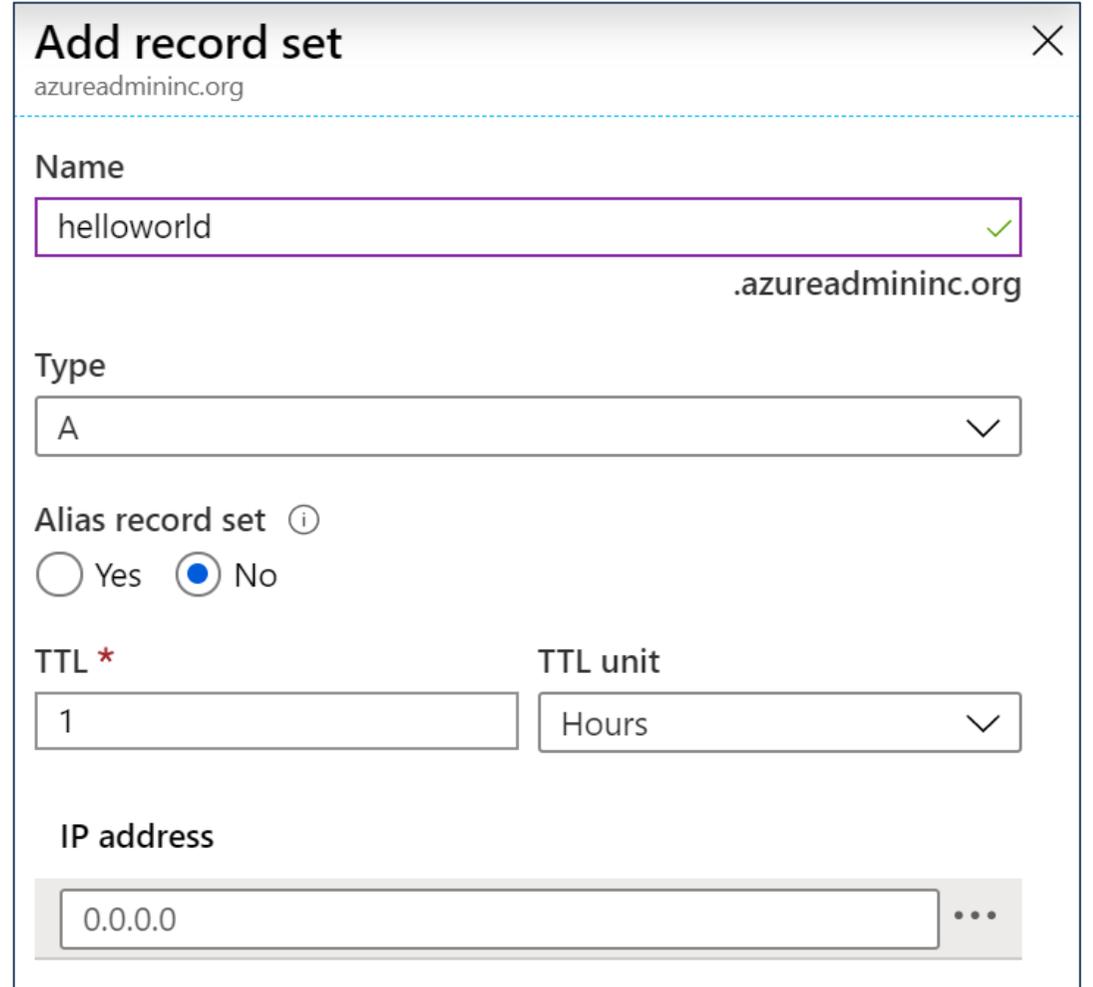
# Dynamically resolve resource name by using alias record

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required



**Add record set** ✕  
azureadmininc.org

Name  
helloworld ✓  
.azureadmininc.org

Type  
A ▼

Alias record set ⓘ  
 Yes  No

TTL \*  TTL unit   
 ▼

IP address  
 ⋮

# Configure a private DNS zone

Use your own custom domain names

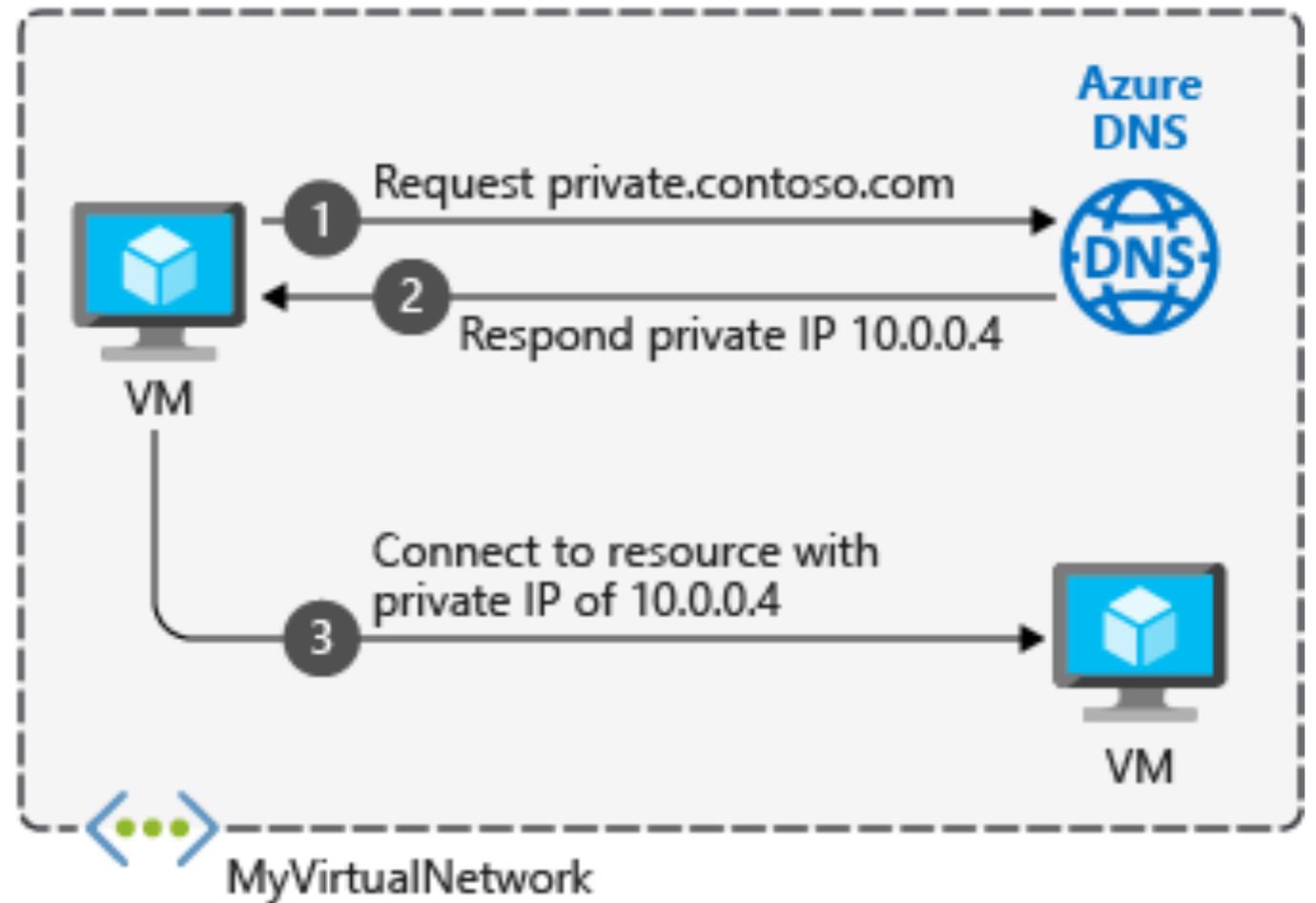
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

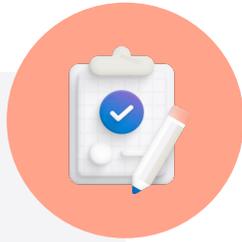
Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



# Learning Recap – Host your domain on Azure DNS



Check your  
knowledge  
questions and  
additional  
study

## Reference modules

- [Introduction to Azure DNS](#)
- [Host your domain on Azure DNS](#)

# Lab – Implement Virtual Networks



# Lab 04 – Implement Virtual Networking



This lab is the first of three labs that focus on virtual networking. In this lab, you learn the basics of virtual networking and subnetting. You learn how to protect your network with Network Security Groups and Application Security Groups. You learn how to configure Azure DNS.

## Job Skills

**Task 1:** Create a virtual network with subnets using the portal.

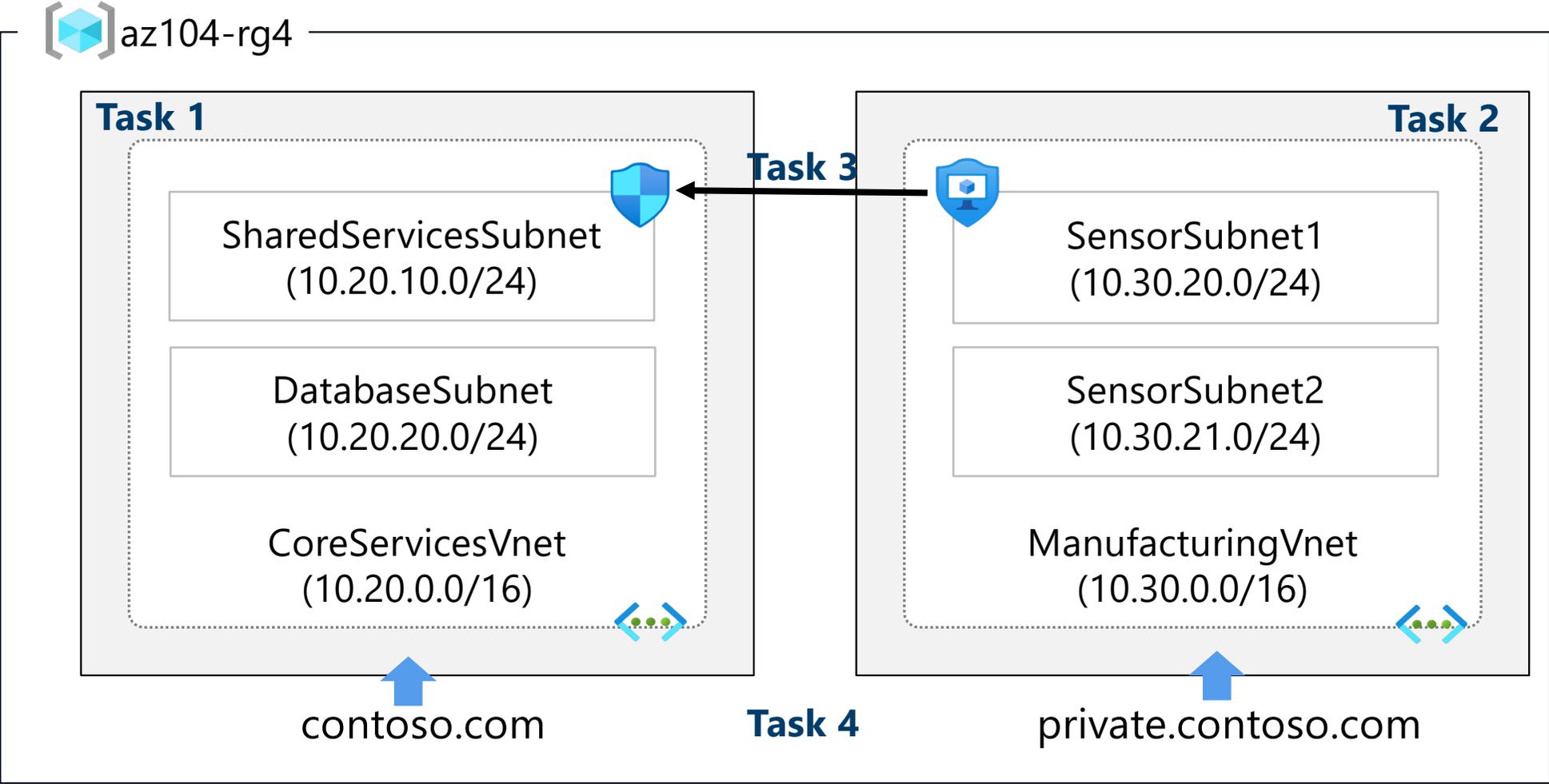
**Task 2:** Create a virtual network and subnets using a template.

**Task 3:** Create and configure communication between an Application Security Group and a Network Security Group.

**Task 4:** Configure public and private Azure DNS zones.

Next slide for an architecture diagram 

# Lab 04 – Architecture diagram



End of presentation

