

AZ-104

Administer Virtual Networking



AZ-104 Course Outline

01: Administer Identity

02: Administer Governance and Compliance

03: Administer Azure Resources

04: Administer Virtual Networking

05: Administer Intersite Connectivity

06: Administer Network Traffic Management

07: Administer Azure Storage

08: Administer Azure Virtual Machines

09: Administer PaaS Compute Options

10: Administer Data Protection

11: Administer Monitoring

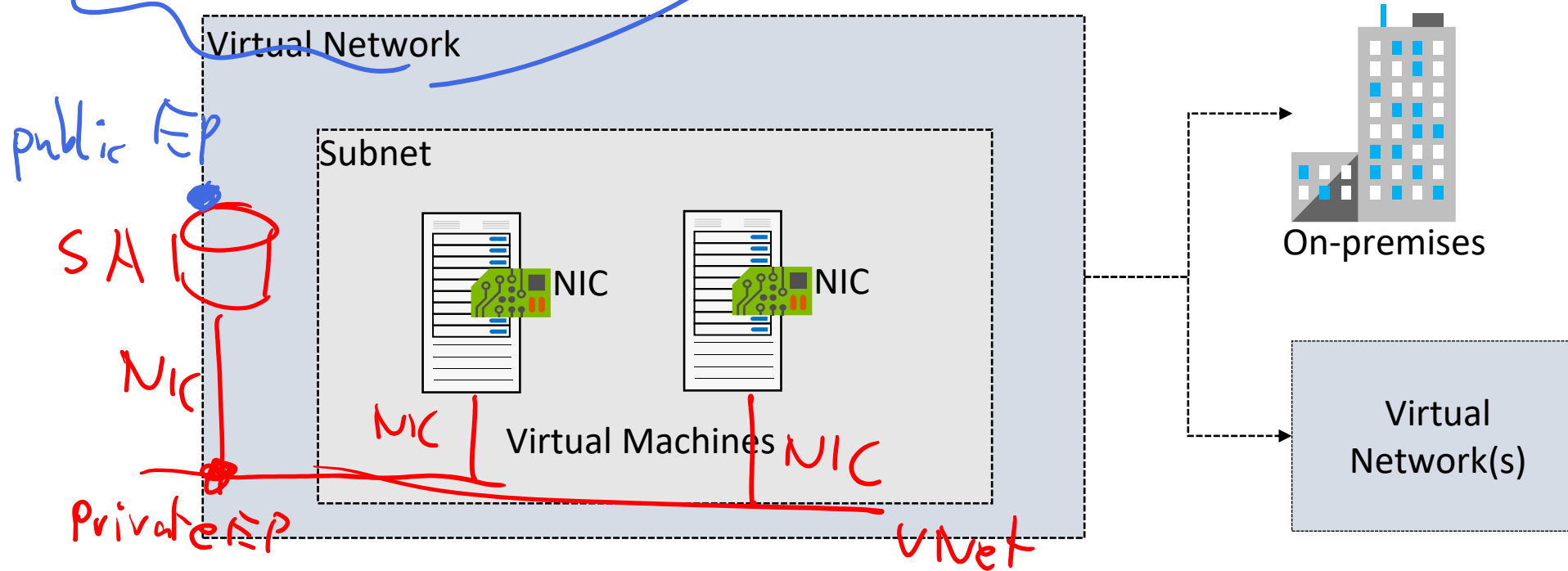
Learning Objectives - Administer Virtual Networking

- [Configure Virtual Networks](#)
- [Configure Network Security Groups](#)
- [Configure Azure DNS](#)
- [Lab 04 – Implement Virtual Networks](#)

Configure Virtual Networks



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 on subnet
- Check for overlapping address paces

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	-

Azure Firewall Subnet

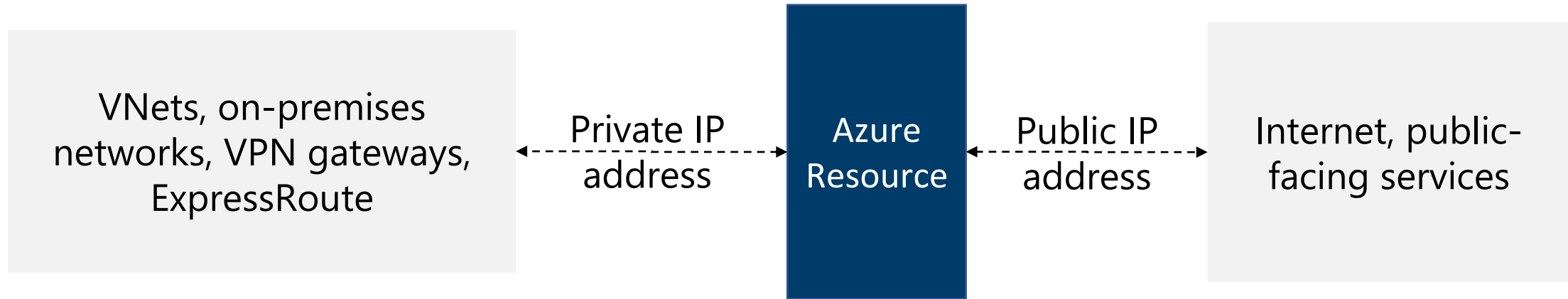
A virtual network can be segmented into one or more subnets

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

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Dynamic vs Static

Microsoft vs. internet routing

[Home](#) > [Public IP addresses](#) >

Create public IP address ...

[Basics](#) [Tags](#) [Review + create](#)

Configuration details

Name *

The name must not be empty.

IP Version * ⓘ ☒ IPv4 ☐ IPv6

SKU * ⓘ ☐ Basic ☒ Standard

Availability zone * ⓘ

Tier * ⓘ ☐ Global ☒ Regional

IP address assignment * ⓘ ☐ Dynamic ☒ Static

Routing preference * ⓘ ☒ Microsoft network ☐ Internet

Idle timeout (minutes) * ⓘ

DNS name label ⓘ

Associate Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

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

Configure Network Security Groups (NSGs)





Implement Network Security Groups


 **nsg0**
Network security group


 Directory: Microsoft


→ Move


 Delete


 Refresh

 Overview

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems

Resource group [\(change\)](#) : rg01

Location : East US

Subscription [\(change\)](#) :

Subscription ID :

Tags [\(change\)](#) : [Click here to add tags](#)

Custom security rules : 1 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

⌵

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

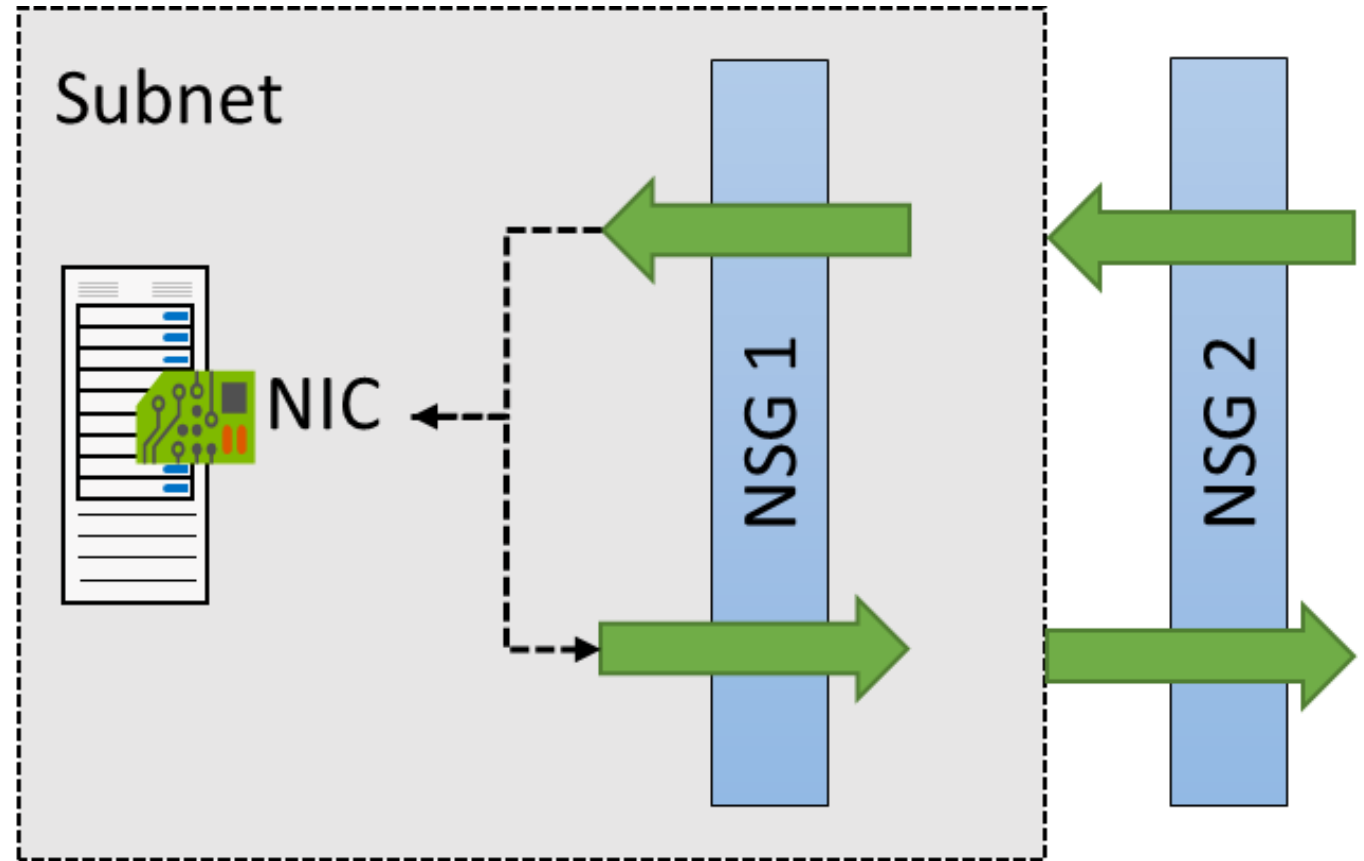
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

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

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

8080

Protocol

☒ Any ☐ TCP ☐ UDP ☐ ICMP

Action

☒ Allow ☐ Deny

Priority * ⓘ

1016 ✓

Name *

AllowAnyCustom8080Inbound

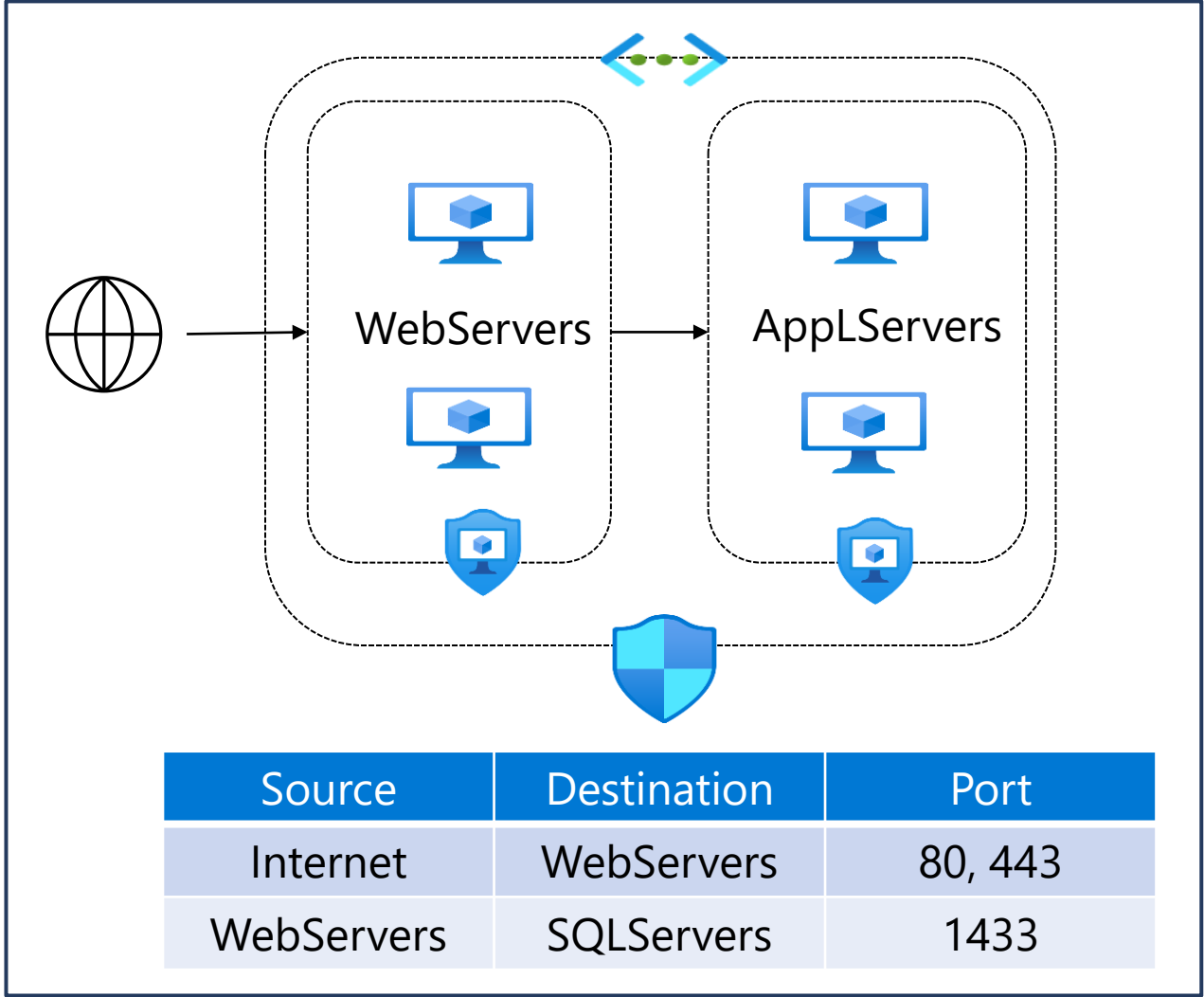
Implement Application Security Groups

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



Configure Azure DNS



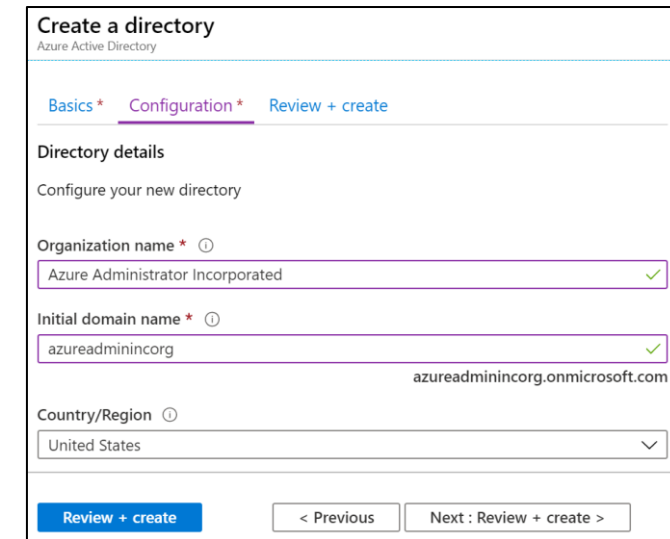
Identity Domains and Custom Domains

When you create a new AAD Tenant, a new default domain is created

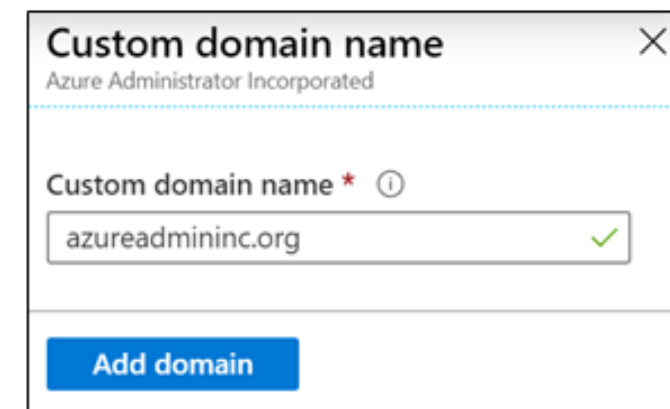
The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can customize/change the name

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



The screenshot shows the 'Create a directory' page in the Azure Active Directory portal. The 'Configuration' tab is selected, showing fields for 'Organization name' (Azure Administrator Incorporated), 'Initial domain name' (azureadminincorg), and 'Country/Region' (United States). The 'Initial domain name' field is highlighted with a green checkmark, and the full domain name 'azureadminincorg.onmicrosoft.com' is displayed below it. Navigation buttons include 'Review + create', '< Previous', and 'Next : Review + create >'.



The screenshot shows the 'Custom domain name' dialog box. The 'Custom domain name' field is filled with 'azureadmininc.org' and has a green checkmark next to it. The 'Add domain' button is visible at the bottom.

Create Azure DNS Zones

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 * MSDN Platforms Subscription

Resource group * rg-dns

[Create new](#)

Instance details

Name * azureadmininc.org

Resource group location ⓘ East US

Review + create


Previous

Next : Tags >

[Download a template for automation](#)

Delegate DNS Domains

- 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

 **azureadmininc.org**
DNS zone

[+ Record set](#) [→ Move](#) [🗑 Delete zone](#) [🔄 Refresh](#)

Resource group (change) rg-dns	Name server 1 ns1-02.azure-dns.com.
Subscription (change) MSDN Platforms Subscription	Name server 2 ns2-02.azure-dns.net.
Subscription ID	Name server 3 ns3-02.azure-dns.org.
	Name server 4 ns4-02.azure-dns.info.
Tags (change) Click here to add tags	

Add DNS Record Sets

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 *

1

TTL unit

Hours

✓

IP address

0.0.0.0

...

Plan for Private DNS Zones

Use your own custom domain names

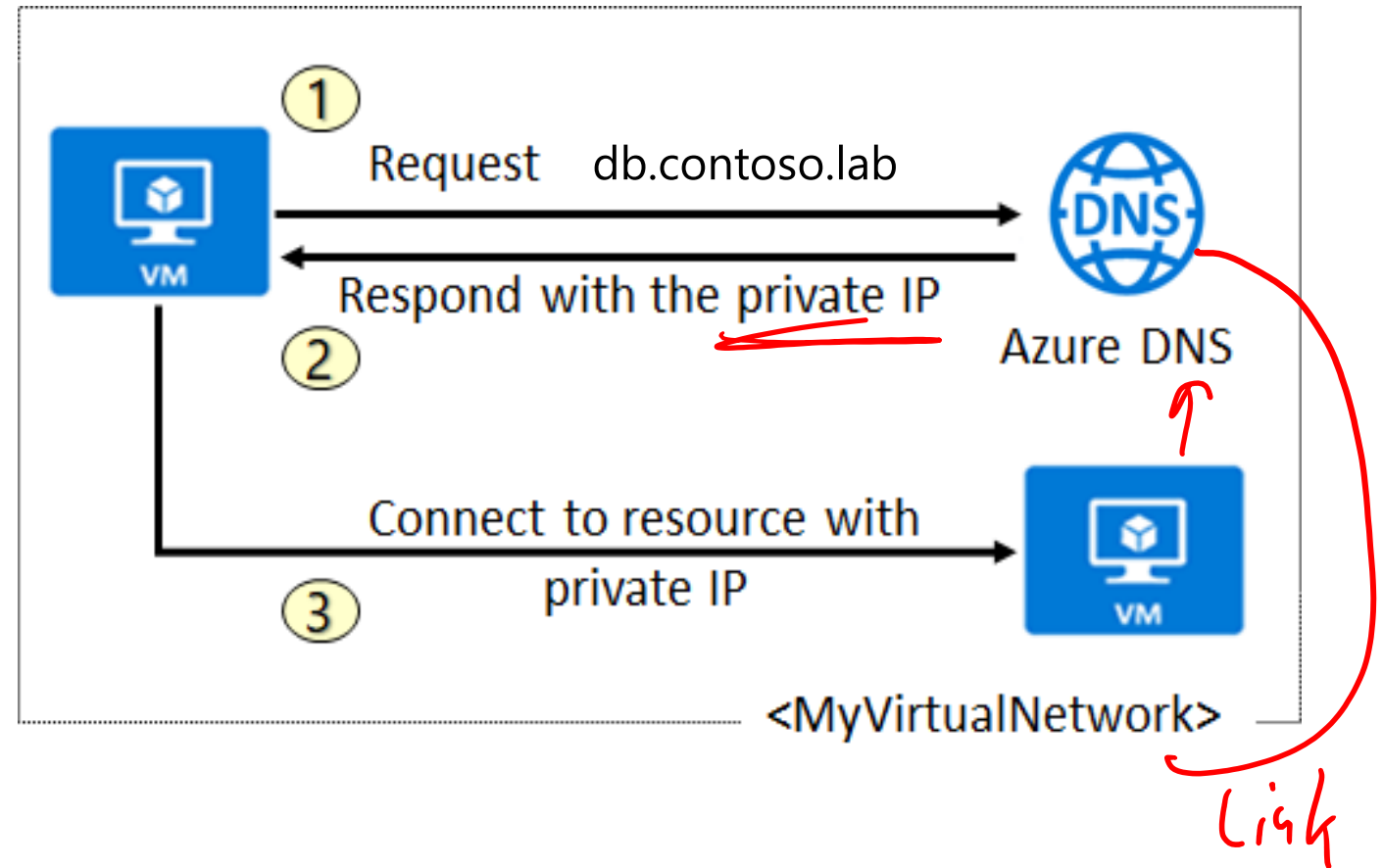
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Demonstration - DNS

- Create a DNS zone
- Add a DNS record set
- View the name servers



Lab – Implement Virtual Networks



Lab 04 – Implement Virtual Networking



You plan to create a virtual network in Azure that will host a couple of Azure virtual machines. You will deploy them into different subnets and must ensure their IP addresses will not change over time. For security requirements, you need to protect public endpoints of Azure virtual machines accessible from Internet. Finally, you need to implement DNS name resolution.

Objectives

Task 1: Create and configure a virtual network

Task 2: Deploy virtual machines into the virtual network

Task 3: Configure private and public IP addresses of Azure virtual machines

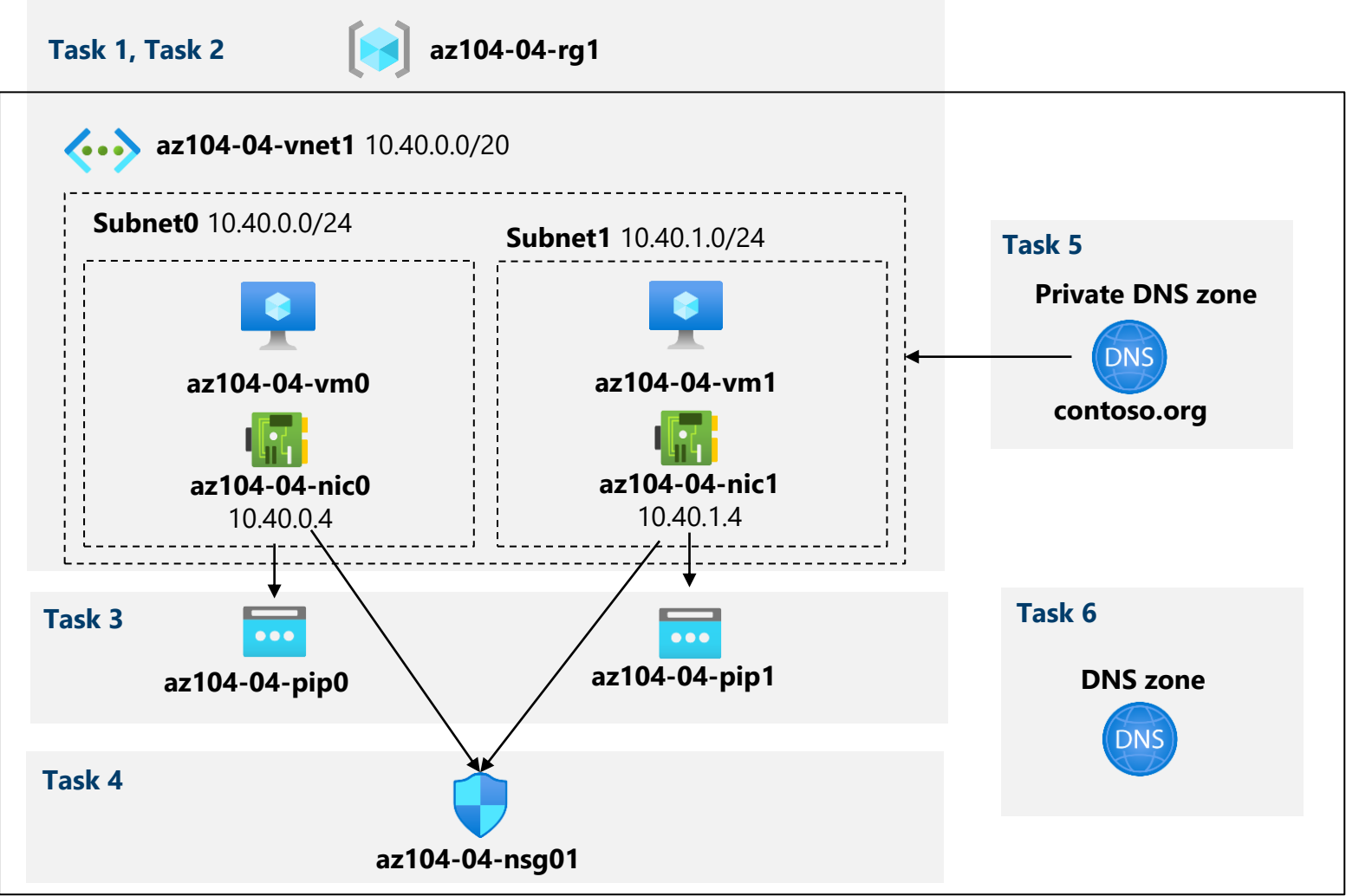
Task 4: Configure network security groups

Task 5: Configure Azure DNS for internal name resolution

Task 6: Configure Azure DNS for external name resolution

Next slide for an architecture diagram 

Lab 04 – Architecture diagram



End of presentation

