Azure Multi-VNet Infrastructure Workshop Guide

Task I - Create Virtual Networks and VNet Peering

Step 1: Create EastUS VNet

1. Navigate to **Virtual networks** in Azure Portal
2. Click **+ Create**
3. **Basics Tab:**
   - Resource group: Create new `EastUS-RG`
   - Name: `EastUS-VNet`
   - Region: `East US`
4. **IP Addresses Tab:**
   - Address space: `10.1.0.0/16`
   - Add subnet: `Web-Subnet` - `10.1.1.0/24`
   - Add subnet: `GatewaySubnet` - `10.1.255.0/27`
5. Click **Review + create** → **Create**

Step 2: Create EastUS2 VNet

1. Navigate to **Virtual networks** in Azure Portal
2. Click **+ Create**
3. **Basics Tab:**
   - Resource group: Create new `EastUS2-RG`
   - Name: `EastUS2-VNet`
   - Region: `East US 2`
4. **IP Addresses Tab:**
   - Address space: `10.2.0.0/16`
   - Add subnet: `Server-Subnet` - `10.2.1.0/24`
   - Add subnet: `GatewaySubnet` - `10.2.255.0/27`
5. Click **Review + create** → **Create**

Step 3: Configure VNet Peering

1. Go to **EastUS-VNet** → **Settings** → **Peerings**
2. Click **+ Add**
3. **This virtual network:**
   - Peering link name: `EastUS-to-EastUS2`

- Allow virtual network access: **Enabled**

4. **Remote virtual network:**
   - Peering link name: `EastUS2-to-EastUS`
   - Virtual network: Select `EastUS2-VNet`
   - Allow virtual network access: **Enabled**
5. Click **Add**
6. Verify both peerings show **Connected** status

Task II - Deploy Virtual Machines

Step 4: Create Availability Set

1. Navigate to **Availability sets** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS-RG`
   - Name: `WebServers-AS`
   - Region: `East US`
   - Fault domains: `2`
   - Update domains: `5`
3. Click **Review + create** → **Create**

Step 5: Deploy Web Server VMs (W1 and W2)

Create W1 VM:

1. Navigate to **Virtual machines** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS-RG`
   - VM name: `W1-WebServer`
   - Region: `East US`
   - Availability options: `Availability set`
   - Availability set: `WebServers-AS`
   - Image: `Windows Server 2022 Datacenter`
   - Size: `Standard_B2s`
   - Username: `azureuser`
   - Password: Create secure password
3. **Networking:**

- Virtual network: `EastUS-VNet`
- Subnet: `Web-Subnet`
- Public IP: Create new
- NIC network security group: `Basic`
- Public inbound ports: `RDP (3389), HTTP (80), HTTPS (443)`

4. Click **Review + create** → **Create**

Create W2 VM:

1. Repeat above steps with:
   - VM name: `W2-WebServer`
   - Same availability set: `WebServers-AS`
   - Same network settings

Step 6: Deploy WS11 Server

1. Navigate to **Virtual machines** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS2-RG`
   - VM name: `WS11-Server`
   - Region: `East US 2`
   - Image: `Windows Server 2022 Datacenter`
   - Size: `Standard_B2s`
   - Username: `azureuser`
   - Password: Create secure password
3. **Networking:**
   - Virtual network: `EastUS2-VNet`
   - Subnet: `Server-Subnet`
   - Public IP: `None`
   - NIC network security group: `Basic`
   - Public inbound ports: `None`
4. Click **Review + create** → **Create**

Step 7: Configure Load Balancer

1. Navigate to **Load balancers** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS-RG`

- Name: `WebServers-LB`
- Region: `East US`
- SKU: `Standard`
- Type: `Public`

3. **Frontend IP configuration:**
   - Name: `LoadBalancerFrontEnd`
   - IP type: `IP address`
   - Public IP address: Create new `LB-PublicIP`
4. **Backend pools:**
   - Name: `WebServers-Pool`
   - Virtual network: `EastUS-VNet`
   - Add both W1 and W2 VMs
5. **Inbound rules:**
   - Type: `Load balancing rule`
   - Name: `HTTP-Rule`
   - Protocol: `TCP`
   - Port: `80`
   - Backend port: `80`
6. **Health probes:**
   - Name: `HTTP-Probe`
   - Protocol: `HTTP`
   - Port: `80`
   - Path: `/`
7. Click **Review + create** → **Create**

Step 8: Setup RD Gateway

1. RDP to W1 VM using public IP
2. Install **Remote Desktop Services** role:
   - Server Manager → **Add Roles and Features**
   - Select **Remote Desktop Services**
   - Choose **Remote Desktop Gateway**
   - Complete installation
3. Configure RD Gateway:
   - RD Gateway Manager → **Properties**

- Set up SSL certificate
- Configure user access policies

4. Configure firewall rules for RD Gateway ports

Step 9: Configure Azure Firewall for WS11

1. Navigate to **Firewalls** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS2-RG`
   - Name: `EastUS2-Firewall`
   - Region: `East US 2`
   - Firewall SKU: `Standard`
   - Virtual network: `EastUS2-VNet`
   - Public IP: Create new
3. **Application Rules:**
   - Rule collection name: `Block-SocialMedia`
   - Priority: `100`
   - Action: `Deny`
   - Rules:
     - Name: `Block-Facebook`
     - Source: `10.2.1.0/24`
     - Target FQDNs: `*.facebook.com`, `*.instagram.com`
     - Name: `Block-Twitter`
     - Source: `10.2.1.0/24`
     - Target FQDNs: `*.twitter.com`, `*.x.com`
4. Create and associate route table to redirect WS11 traffic through firewall

Task III - Implement Secure Connectivity

Step 10: Configure VPN Gateway

1. Navigate to **Virtual network gateways** → **+ Create**
2. **Create for EastUS VNet:**
   - Name: `EastUS-VPN-Gateway`
   - Region: `East US`
   - Gateway type: `VPN`
   - VPN type: `Route-based`

- SKU: `VpnGw1`
- Virtual network: `EastUS-VNet`
- Public IP: Create new

3. **Create for EastUS2 VNet:**
   - Name: `EastUS2-VPN-Gateway`
   - Region: `East US 2`
   - Same settings as above
   - Virtual network: `EastUS2-VNet`
4. **Create VNet-to-VNet Connection:**
   - Go to EastUS VPN Gateway → **Connections**
   - Add VNet-to-VNet connection
   - Connect to EastUS2 VPN Gateway
   - Set shared key
   - Repeat from EastUS2 gateway

Step 11: Configure Network Security Groups

Web Servers NSG:

1. Navigate to **Network security groups** → **+ Create**
2. Name: `WebServers-NSG`
3. **Inbound rules:**
   - Allow HTTP (80) from Internet
   - Allow HTTPS (443) from Internet
   - Allow RDP (3389) from specific admin IPs
   - Allow traffic from EastUS2 VNet (10.2.0.0/16)
4. Associate with Web-Subnet

WS11 Server NSG:

1. Create NSG: `WS11-NSG`
2. **Inbound rules:**
   - Allow traffic from EastUS VNet (10.1.0.0/16)
   - Deny all other inbound traffic
3. **Outbound rules:**
   - Allow to EastUS VNet
   - Route through Azure Firewall for internet access

4. Associate with Server-Subnet

Task IV - Setup Storage Solutions

Step 12: Configure EastUS Storage (ZRS)

1. Navigate to **Storage accounts** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS-RG`
   - Name: `eastusstorageXXXX` (unique name)
   - Region: `East US`
   - Performance: `Standard`
   - Redundancy: `Zone-redundant storage (ZRS)`
3. **Access Control (IAM):**
   - Add role assignments for RBAC
   - Assign appropriate roles to users/applications
4. **Shared Access Signatures:**
   - Navigate to **Shared access signature**
   - Configure permissions and expiry
   - Generate SAS token and URL
5. **Access Keys:**
   - Navigate to **Access keys**
   - Copy key1 and connection string

Step 13: Configure EastUS2 Storage (GRS)

1. Navigate to **Storage accounts** → **+ Create**
2. **Basics:**
   - Resource group: `EastUS2-RG`
   - Name: `eastus2storageXXXX` (unique name)
   - Region: `East US 2`
   - Performance: `Standard`
   - Redundancy: `Geo-redundant storage (GRS)`
3. **File Shares:**
   - Navigate to **File shares** → **+ File share**
   - Name: `ws11-share`
   - Tier: `Standard`

4. **Connect to WS11:**
   - RDP to WS11 server
   - Open PowerShell as Administrator
   - Use the connection script from Azure portal:

     ```
     powershell

     net use S: \\storageaccount.file.core.windows.net\ws11-share /persistent:yes
     ```

   - Enter storage account credentials when prompted

Step 14: Verify and Test Setup

1. **Test VNet Connectivity:**
   - From W1/W2, ping WS11 private IP
   - From WS11, test connection to web servers
2. **Test Load Balancer:**
   - Access load balancer public IP
   - Verify traffic distributes between W1 and W2
3. **Test RD Gateway:**
   - Connect using RD Gateway from external client
4. **Test Storage:**
   - Verify S: drive mapping on WS11
   - Test file operations on mounted drive
5. **Test Firewall Rules:**
   - From WS11, attempt to access blocked social media sites
   - Verify access is denied

Workshop Completion Checklist

- [ ] EastUS VNet created with proper subnets
- [ ] EastUS2 VNet created with proper subnets
- [ ] VNet peering established and connected
- [ ] W1 and W2 VMs deployed in availability set
- [ ] WS11 VM deployed in EastUS2
- [ ] Load balancer configured and distributing traffic
- [ ] RD Gateway configured for remote access
- [ ] Azure Firewall blocking social media access
- [ ] VPN Gateway connections established
- [ ] NSGs configured and applied

- [ ] ZRS storage configured in EastUS with access methods
- [ ] GRS storage configured and mapped to S: drive on WS11
- [ ] All connectivity and security tests passed