Azure Cloud Project Guidelines

Professor: Asghar Ghori

Project Overview

This capstone project simulates several common real-world Azure tasks cloud architects, engineers, and administrators perform. The project challenges learners to apply their Azure knowledge and technical skills gained from the bootcamp to build a highly available, scalable, and secure infrastructure using a variety of Azure services, resources, and features across multiple availability zones in two Azure regions. Learners are expected to use the Azure Portal to complete the project. They may also need to use AZ CLI and/or PowerShell to supplement the Azure portal.

Technical Skills Assessed

Azure services, resources, and features assessed in the project include:

- Identity and Access (Azure Active Directory)
- Governance and Compliance (management groups, Azure Policy, tags, etc.)
- Networking (virtual networks, subnets, peering, etc.)
- Security (network security groups, etc.)
- Storage (storage accounts, Azure Files, blob containers, etc.)
- Compute (Windows/Linux virtual machines, managed disks, container instances)
- Network Traffic Management (load balancers, etc.)
- Data Protection (backups, policies)
- Monitoring (Azure Monitor)
- Cost Management (cost analysis, budgeting, reporting, etc.)
- Azure Interfaces (Portal, AZ CLI, PowerShell)

Soft Skills Assessed

- Critical thinking
- Researching
- Troubleshooting
- Problem-solving
- Decision-making
- Self-judgement
- Organization
- Stress management
- Independent and collaborative working

Project Requirements

Use a free-tier or pay-as-you-go Azure account to accomplish the project deliverables.

Project Cost

The Microsoft cost for the implementation of this Azure project should not surpass **$20** if the entire deployment is performed over **5 consecutive days**.

Recommendations

Implement the project in region 1 (Australia East) and region 2 (UK South). If either of these regions show VM sizes as unavailable, search for other regions that do not have that issue and use those instead.

Instructions

1. Append your ***HumberID*** when naming resources (users, groups, resource groups, virtual networks, subnets, management groups, policy initiatives, virtual machines, storage accounts, containers, Azure Files, load balancers, etc.).
2. Stick to the default values or change them only if asked or required for a successful implementation.

Deliverables

1. Take screenshots or short videos, or a combination, where indicated, and add them to a Word document in the order in which they are requested along with an appropriate heading.
2. Create an architecture diagram in Microsoft PowerPoint (or any other tool of your choice such as Microsoft Visio, draw.io, etc.) using the Azure stencil library available for free **here**. The architecture diagram must clearly depict the (a) hub-and-spoke network topology, (b) all the services used, (c) resources implemented, and (d) their relationships and connections. This should include management group, subscriptions, resource groups, virtual networks, subnets, peering connection, availability sets, virtual machines, storage account, file share, private endpoint, recovery services vault, backups, etc. The diagram must also be (e) scalable to accommodate future growth in the environment. **Note 1:** Do not show NICs in the diagram. **Note 2:** Copied and pasted Azure Visualizer images are not acceptable.
3. Attach both files (your project document and the architecture diagram) under Azure Project in Blackboard and submit.

Rubric and Passing Marks

The following rubric will be used to grant marks to project work. Each task under Project Details has maximum marks shown in parentheses. The Hands-On Implementation section is worth **78** marks and the Diagram and Presentation sections **10** and **12** marks, respectively.

Hands-On Implementation	**Max Marks**	**Your Marks**
Establish AAD Access	5	
Establish AAD Access (**-10** negative marks if the new user account is not used to complete rest of the project work)	-10	
Add Subscriptions	3	
Create Resource Groups	2	
Configure Networking – vnet1	6	
Configure Networking – vnet2 and peering	8	
Configure Governance	8	
Create Storage	2	
Build Compute Resources for Windows	8	
Create and Attach Public IP Addresses	1	
Build Compute Resources for Linux	9	
Create File Share and Mount it to Windows	4	
Configure Load Balancer	6	
Test Load Balancer and Web Server Functionalities	5	
Create Data Disk and Mount it to Linux	4	
Configure Backups	4	
Use Azure Container Instances	3	
Sub-Total	**78**	
Diagram		
Architecture Diagram (see #2 under deliverables above).	10	
Sub-Total	**10**	
Presentation		
Presentation: - Originality (3) - Clarity (3) - Relevance (3) - Answering applicable technical questions (3)	12	
Sub-Total	**12**	
GRAND TOTAL	**100**	

Warning

Copying and pasting other student's work and submitting it as one's own is a serious academic misconduct. All involved parties will get a ZERO, no exceptions.

Feedback

We look forward to receiving your constructive feedback in terms of project flow, errors encountered, fixes you applied to make things functional, and so on. Please record your comments where they apply in your project document.

Project Details

Establish AAD Access

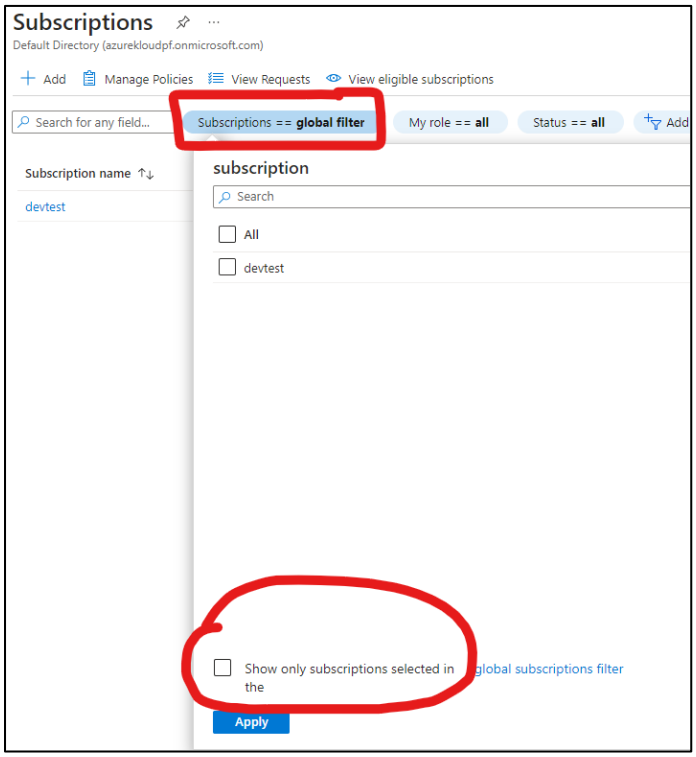
1. Create an AAD user called ***HumberID*** (1) [***HumberID*** is your student ID]
2. Provide **Global Administrator** role to the user (1)
3. Create a group called ***HumberID*-grp** with group type **Security** and membership type **Assigned** (1). Add user ***HumberID*** to this group both as a member and owner (2).
4. Log out and log back in as the new user ***HumberID***
5. Perform the rest of the project work as this user (**-10** negative marks if this user is not used to complete rest of the project work)

1 SCREENSHOT showing the new user and the assigned role
1 SCREENSHOT showing the new group and its membership

Add Subscriptions

6. Add one new pay-as-you-go subscription called **sub-a** (1)
7. Add another pay-as-you-go subscription called **sub-b** (1). **You may have to deploy some resources in sub-a, and then wait for a day or two before you are allowed to create sub-b. Refer to this Microsoft article.**
8. Assign the Owner RBAC role to user ***HumberID*** on scopes **sub-a** and **sub-b** (1)

WARNING: If you do not see all your subscriptions, untick "Show only subscriptions selected in the global subscription filter", and click Apply. See image below:



Create Resource Groups

9. Create a resource group called **RG1-*HumberID*** in region 1 in **sub-a** (1). All resources for **sub-a** must be created in this region.
10. Create a resource group called **RG2-*HumberID*** in region 2 in **sub-b** (1). All resources for **sub-b** must be created in this region.

2 SCREENSHOTS (one per resource group) showing the Overview blade

Configure Networking – vnet1

11. In **RG1-*HumberID*** under **sub-a**, create networking resources as follows:
    a. Virtual network name and CIDR: **vnet1** with CIDR 10.10.0.0/23 (1)
    b. Subnet 1 name and CIDR: **vnet1-subnet1** with CIDR 10.10.0.0/24 (1)
    c. Subnet 2 name and CIDR: **vnet1-subnet2** with CIDR 10.10.1.0/24 (1)
    d. Remove the default subnet if it exists
    e. NSG name and rules: **vnet1-nsg** with three inbound allow rules for RDP (port 3389), HTTP (port 80), and SMB (port 445) protocols (1)
    f. Attach the NSG to both subnets (2)

3 SCREENSHOTS showing the Overview, Address space, and Subnets blades of the virtual network

2 SCREENSHOTS showing the Overview and Subnets blades of the network security group

Configure Networking – vnet2 and peering

12. In **RG2-*HumberID*** under **sub-b**, create networking resources as follows:
    a. Virtual network name and CIDR: **vnet2** with CIDR 10.20.0.0/23 (1)
    b. Subnet 1 name and CIDR: **vnet2-subnet1** with CIDR 10.20.0.0/24 (1)
    c. Subnet 2 name and CIDR: **vnet2-subnet2** with CIDR 10.20.1.0/24 (1)
    d. Remove the default subnet if it exists
    e. NSG name and rules: **vnet2-nsg** with one inbound allow rule for SSH (port 22) access (1)
    f. Attach the NSG to both subnets (2)
13. Establish peering between **vnet1** and **vnet2** (2)

2 SCREENSHOTS showing the Overview and Subnets blades of the virtual network

2 SCREENSHOTS showing the Overview and Subnets blades of the network security group

Hint: Use **this** IP calculator if required

Configure Governance

14. Create a management group called **governance** and add both subscriptions to it (1)

1 SCREENSHOT showing the management group hierarchy

15. Create a custom policy initiative called **project_initiative** and add the following assignments to it:
    a. Enforce an assignment to apply a tag called "environment" and value "project" at the time of each resource creation (2). Use the "Require a tag and its value on resources" built-in policy.
    b. Enforce an assignment to restrict the allowed locations for resource group creation to region 1 and region 2 only (2). Use the "Allowed locations" built-in policy.
16. Assign the **project_initiative** to the management group (1)
17. Wait for 30 minutes after the initiative assignment for the policies to take effect.
18. Make sure that all the resources you create going forward are compliant with the **project_initiative** (2)

2 SCREENSHOTS showing Compliance and Assignments from Azure Policy
1 SCREENSHOT showing the list of policies in the initiative
2 SCREENSHOTS showing definitions for both policies

Create Storage

19. Create one general-purpose LRS storage account called ***HumberID*storage1** in **sub-a** (1)
20. Create one general-purpose LRS storage account called ***HumberID*storage2** in **sub-b** (1)

2 SCREENSHOTS (one per storage account) showing the Overview blade

Build Compute Resources for Windows

21. In **RG1-*HumberID***, create 2 virtual machines using the following configuration:
    a. Hostnames: ***HumberID*-w-vm1** and ***HumberID*-w-vm2** (2)
    b. Operating system: Windows Server 2019 (1)
    c. VM size: D2s_v4 (you may use any other D class VM size)
    d. Vnet/subnet: VM1 (vnet1/subnet1**)**, VM2 **(**vnet1/subnet2**)** (1)
    e. Availability set name: **windows-avs** (1)
    f. Username: your ***HumberID*** and password
    g. VM extensions: "Microsoft Antimalware" (1)
    h. Boot diagnostics: enabled and stored in ***HumberID*storage1** (1)
    i. Public IP: no

Create and Attach Public IP Address Resources

22. In **RG1-*HumberID***, create 2 zone-redundant **standard** SKU public IP address resources called ***HumberID*-w-vm1-pip** and ***HumberID*-w-vm2-pip** with DNS labels ***HumberID*-w-vm1** and ***HumberID*-w-vm2** and attach them to their respective Windows VMs (2).

6 SCREENSHOTS (3 per VM) showing the Overview, Networking, and Serial Console blades of each VM (make sure that Overview also includes Availability and Extensions information)

Build Compute Resources for Linux

23. In **RG2-*HumberID***, create 2 virtual machines using the following configuration:
    a. Hostnames: ***HumberID*-u-vm1** and ***HumberID*-u-vm2** (2)
    b. DNS Name: ***HumberID*-u-vmX** (1)
    c. Operating system: Ubuntu Server 20.04 (1)
    d. VM size: B1ms (you may use any other B class VM size)
    e. Vnet/subnet: VM1 (vnet2/subnet1**)**, VM2 **(**vnet2/subnet2**)** (1)
    f. Public IP: yes, use Basic SKU (1)
    g. Availability set name: **linux-avs** (1)
    h. Username: your ***HumberID*** with SSH keys
    i. VM extensions: "Network Watcher Agent for Linux" (1)
    j. Boot diagnostics: enabled and stored in ***HumberID*storage2** (1)

6 SCREENSHOTS (3 per VM) showing the Overview, Networking, and Serial Console blades (make sure that Overview also includes Availability and Extensions information)

Create File Share and Mount it to Windows

24. Create a file share called ***HumberID*-share1** in ***HumberID*storage1** (1)
25. Create a private endpoint to ***HumberID*-share1** (1)
26. Using the RDP protocol, log on to the VM using its public IF or FQDN, and mount ***HumberID*-share1** to ***HumberID*-w-vm1** as Z: drive using the **private IP address** of the private link (1)
27. Create a file called ***HumberID*** in the Z: drive (1)

1 SCREENSHOT showing the File Share under Azure Storage Account | File Shares
1 SCREENSHOT showing the Overview blade of the private endpoint
1 SCREENSHOT showing the IP Configurations blade of the private endpoint network interface
1 SCREENSHOT showing the Z: drive mounted on Windows VM (log in to the VM)

Configure Load Balancer

28. Create a public load balancer called ***HumberID*-lb1** with both Windows VMs in the backend pool (2)
29. Configure health probes and define load balancing rules. Use your knowledge for this step. (2)
30. Configure web service on both Windows VMs (2)

3 SCREENSHOTS showing the Overview, Frontend IP Configuration, and Backend Pools blades from Azure Load Balancer
2 SCREENSHOTS showing the Health Probes and Load Balancing Rules configuration from Azure Load Balancer

Test Load Balancer and Web Server Functionalities

31. Use the public IP address of Windows VMs one at a time in a browser window to test web server functionality (1)
32. Enter the load balancer public IP in a browser window. Refresh the browser window and ensure web server alternates. (1)
33. Stop VM1 and refresh the browser window a couple of times. You should only see the VM2 page. (1)

34. Start VM1 and stop VM2. Wait for a minute and refresh the browser window for a couple of times. You should only see the Windows VM1 page. (1)
35. Start VM2. Wait for a minute and refresh the browser window for a few times. You should see the two web servers alternating. (1)

(VIDEO showing 31 to 35)

Create Data Disk and Mount it to Linux

36. Create a managed disk of size 10GB and attach it to Linux VM1 (1)
37. Log in to the Linux VM using the SSH protocol and use any tool to create a 10GB file system on the new disk (1) and mount it persistently (1) at **/mydisk01** mount point (1). Acceptable file system size is between 8GB and 10GB.

1 SCREENSHOT showing the Overview blade of the data disk from Azure Disks
3 SCREENSHOTS showing the outputs of "**lsblk**, "**cat /etc/fstab**", and "**df -h**" commands (log in to the Linux VM is required)

Configure Backups

38. Create a recovery services vault called ***HumberID*-rsv1** in region 1 (1)
39. Create a backup policy called ***HumberID*-daily** to run 6:00 am every day with a snapshot retention for 1 day and daily backup points for 8 days. (1)
40. Add both Windows VMs to the recovery services vault and enable backups (1)
41. Run initial backups for both VMs (1)

1 SCREENSHOT1 showing Backup Center | Backup Instances
1 SCREENSHOT1 showing Backup Center | Backup Policies | *HumberID*-daily

Use Azure Container Instances

42. Use Azure Container Instance service and build a container called ***HumberID*-aci1** in region 2 (1) using a Hello World container image from Azure container registry (1). The DNS label for the container must be ***HumberID*-aci1** (1).

1 SCREENSHOT showing the Overview blade of Azure Container Instance
1 SCREENSHOT showing the web page when the DNS label is entered in a browser window

End of Project

Please destroy all the resources you have created for this project after you have submitted it.