A screenshot of a computer

AI-generated content may be incorrect.

Global VNET peering is the resource of Azure that allows connection between VNets in different regions

Although Gateway devices in both regions would do the job, it is more costly and complex and because of that, it isn’t the right answer

A screenshot of a computer

AI-generated content may be incorrect.

You need a place to store all the logs **before** you can retrieve them

A screenshot of a computer

AI-generated content may be incorrect.

IP Flow Verify specifically checks whether a network security rule is blocking traffic

Traffic Analysis provides usage analytics

Next Hop identifies routing paths

Packet Capture collects network traffic for deeper inspection

A screenshot of a questionnaire

AI-generated content may be incorrect.

The answer is two because Azure SQL Database is a PaaS, so it is fully managed by Azure including their backups

You need to create two policies: one for File Shares and one for VMs

You can use the same Recovery Service Vault for both workloads, however the policies have the “policy type” that defines what that policy is back up

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

As the policy is assigned to the Tenant Root Group it applies to **all subscriptions** and **resource groups**. A requirement to create a VM is the existence or the possibility of creation of VNets, otherwise you won’t have a place to put your VMs in.

A screenshot of a question

AI-generated content may be incorrect.

I misunderstood the question: you should spread the workload of the webservers across the 50 VMs that are not accessible from the internet, hence you need to deploy an Internal Load Balancer

A screenshot of a computer

AI-generated content may be incorrect.

You just needed to know that the only Storage Account types that support Archive tier is GenPV2 and Blob Storage (known as **Blob-Only** too”

A screenshot of a computer

AI-generated content may be incorrect.

The internal load balancer is obvious however the app gateway is more interesting: it can handle internal traffic too when accessing it from a VPN tunnel or **ExpressRoute**. It communicates with on-premises servers when they’re connected to a VPN or by Azure ExpressRoute if traffic is allowed

Traffic Manager is like AWS Global Accelerator btw

A screenshot of a computer

AI-generated content may be incorrect.

Import/Export service is used to import LARGE amounts of data to **Blob Storage and Azure Files**

It can also transfer data **FROM** Blob Storage so both ways can be handled here by this service

A screenshot of a questionnaire

AI-generated content may be incorrect.

This question is tricky because it says “.net **core**”. And dotnet core runs in both windows and linux VMs so, if you’re in the same region of the plan you can use it: plan1 and 2 are in the eastus region so they’re usable

A screenshot of a computer

AI-generated content may be incorrect.

I need to study about ADE

1. DM-Crypt for Linux VMs
2. Bitlocker for Windows VMs
3. Integrated with KeyVault
4. Is possible to back up encrypted VMs
5. It only encrypts VMs at rest

A screenshot of a questionnaire

AI-generated content may be incorrect.

Those are the numbers: max of 3 fault domains and 20 update domains for **one** availability set

A screenshot of a survey

AI-generated content may be incorrect.

B1-3: Up to 3 instances

S1-3: Up to 10 instances

P1-3: Up to 30 instances

Isolated tier increase the scale-out capability count to 100 instances

A screenshot of a computer

AI-generated content may be incorrect.

The vault and the VMs must be in the same region

A screenshot of a computer test

AI-generated content may be incorrect.

The problem is with the mismatch, as the tenant was recently created probably, the domain is ending with onmicrosoft.com which is the default domain when a new Azure AD is created

You must change (or verify) what the custom domain on-prem is and set it too on Azure

A screenshot of a questionnaire

AI-generated content may be incorrect.

Only the Azure AD Portal can manage users in a bulk manner

Yes, you can do a bulk operation with PowerShell or Azure CLI within a script, but none of that is built-in

A screenshot of a computer

AI-generated content may be incorrect.

Need to study more of “Azure Firewall”:

FQDN-base rules belong to **Application rule collections**

Network Rule Collections are layer ¾ and are based on IP addresses, ports, and protocols

NAT Rule Collections deal with **translating** traffic from public IP to private IP

Application Rule Collections are layer 7 and let you specify FQDNs

A screenshot of a computer

AI-generated content may be incorrect.

Dumb error: the user has global admin and has created the directory, it is obvious he has the necessary permissions to add new users

A screenshot of a computer error

AI-generated content may be incorrect.

A point-to-site VPN that uses self-signed certificate needs that each client computer have the proper client certificate installed

**Bottom line**: Whether the certificate is self-signed or from a public/enterprise CA, Azure P2S VPN requires each connecting client to possess a valid, matching client certificate chain. The main benefit of a public/enterprise CA is that clients already trust the root, but they **still** need an individual client certificate to actually authenticate.

A screenshot of a computer program

AI-generated content may be incorrect.

Availability Sets CAN’T prevent VMs from a **data center-level failure**

**A screenshot of a computer program

AI-generated content may be incorrect.**

The required SLA is only achieved by Scale Sets with AZs or FDs. Azure guarantees the 99.95 SLA ONLY if you explicitly deploy VMs or VMSS across multiple FDs or AZs

A screenshot of a computer

AI-generated content may be incorrect.

It’s necessary to register the on-prem server: you install the Azure File Sync Agent on the on-prem server, which makes it known to Azure

The sync group is a logical grouping that defines which files from on-prem should be synchronized with a particular File Share

A screenshot of a computer

AI-generated content may be incorrect.

Azure requires a special subnet for that called exactly “**GatewaySubnet**” within the VNET. Without it you cannot deploy a VPN gateway

A screenshot of a computer

AI-generated content may be incorrect.

I feel the answer for this question could be IP Flow Verify too, because it will define if there is the possibility of connection between those two VMs

However, as IP Flow Verify checks the NSG rules, it would not properly check if there would be connectivity **BETWEEN** them, because one of the instances is external of Azure

I think the keyword here is “**between**”

A screenshot of a computer

AI-generated content may be incorrect.

That’s interesting: the loadbalancer has this inbound NAT rule that serves as a port forwarding, so: if the loadbalancer receives traffic in a specific port, it has this port mapped to a specific VM on a specific backend port