# Cloud Services — Azure (25 Questions)

---

### Q1: AKS workloads fail to pull images from Azure Container Registry (ACR) after you enabled a private cluster.

**Answer:**
Private AKS clusters can't pull from ACR unless you create a **private endpoint** for ACR in the AKS VNet or use a linked service principal/managed identity with `AcrPull` role. Also update AKS nodepool NSG to allow traffic to the private endpoint subnet.

**Sample Points:**

- Private endpoint or VNet integration for ACR.
- Assign AcrPull to nodepool identity.
- Update NSG rules for endpoint subnet.

**Example Code:**

```
az acr network-rule add --name myacr --subnet my-subnet-id
az role assignment create --assignee <nodepoolMSI> --role AcrPull
--scope $(az acr show --name myacr --query id -o tsv)
```

---

### Q2: Azure VM boots slowly after enabling Azure Disk Encryption.

**Answer:**
Azure Disk Encryption uses BitLocker/DM-Crypt. Boot delays happen if KEK/BEK retrieval from Key Vault is slow. Ensure Key Vault is in same region, has private endpoint, and VM has MSI with proper Key Vault access.

**Sample Points:**

- Keep Key Vault in same region as VM.
- Private endpoint for speed/security.

- MSI role: `Key Vault Crypto User`.
  **ExampleCode:**

```
az keyvault set-policy --name kvname --object-id <msi>
--key-permissions wrapKey unwrapKey get
```

---

## Q3: Azure Function app fails connecting to Azure SQL DB due to firewall rules.

**Answer:**
Enable **VNetintegration** for the Function App and add the subnet to Azure SQL firewall rules or configure a private endpoint. For security, disable Allow Azure services broad rule.

**SamplePoints:**

- VNet integration + firewall subnet allow.
- Prefer private endpoint for isolation.
- Remove broad "Allow Azure services".
  **Example Code:**

```
az sql server vnet-rule create --name allow-func --server mydbserver
--subnet subnetid
```

---

## Q4: App Service must securely fetch secrets from Key Vault without code changes.

**Answer:**
Enable a **managed identity** for the App Service, grant it `Key Vault Secrets User` role, and use **Key Vault references** in app settings (`@Microsoft.KeyVault(SecretUri=...)`).
**Sample Points:**

- Managed identity avoids static secrets.
- Key Vault references inject values automatically.

- Role: `Key Vault Secrets User`.
  **Example Code:**

```
az webapp identity assign --name myapp --resource-group rg
az keyvault set-policy --name mykv --object-id <msi>
--secret-permissions get list
```

---

## Q5: Azure Storage account with public access was accidentally created. Enforce no-public-storage org-wide.

**Answer:**
Use Azure Policy `Storage accounts shouldrestrictnetworkaccess` and `Public network access should be disabled`. Deny assignments at subscription level.
**Sample Points:**

- Azure Policy enforces at create/update.
- Disable public access in config.
- Scope to subscription for coverage.
  **Example Code:**

```
az policy assignment create --policy
"StorageAccounts_PublicAccess_Disable" --scope /subscriptions/xxxx
```

---

## Q6: VM Scale Set update doesn't roll out new custom script extension to all instances.

**Answer:**
Ensure `upgradePolicy.mode=Automatic` and reapply extension with `--force-update`. For rolling upgrades, check `healthProbe` to avoid unhealthy replacements.
**Sample Points:**

- Automatic upgrade mode.
- Force extension update across instances.

- Health probe gates replacements.
  **Example Code:**

```
az vmss extension set --publisher Microsoft.Azure.Extensions --name
CustomScript --version 2.1 --vmss-name myvmss --resource-group rg
--force-update
```

---

## Q7: AKS ingress TLS cert is not issued via Azure-managed cert.

**Answer:**
Azure-managed certs require public DNS A record to the ingress IP and HTTPS-enabled ingress. Ensure ingress annotation kubernetes.io/ingress.class=nginx and `cert-manager.io/issuer` are correct.

**Sample Points:**

- Public DNS must resolve to LB IP.
- Correct ingress annotations.
- cert-manager status must be `Ready`.
  **Example Code:**

```
kubectl describe certificate my-cert
```

---

## Q8: App Insights logs ingestion cost spiked after verbose debug logging.

**Answer:**
Lower the sampling rate, use severity filters in the SDK, and apply retention policy (e.g., 30 days). Route verbose logs to Blob Storage via diagnostic settings.

**Sample Points:**

- Sampling reduces ingestion.
- Filter at SDK to drop debug logs.
- Archive long-term in Blob.
  **Example Code:**

```
az monitor app-insights component update --app myapp
--sampling-percentage 20
```

---

## Q9: Azure SQL DB performance drops during ETL; DTU consumption maxes out.

**Answer:**
Switch to vCore model for predictable CPU/memory scaling, enable **automatic tuning** for index mgmt, and consider **read scale-out** for read-only ETL queries.
**Sample Points:**

- vCore for flexible scaling.
- Automatic tuning indexes.
- Read scale-out for reporting.
  **Example Code:**

```
az sql db update --name mydb --service-objective GP_Gen5_8
```

---

## Q10: Application Gateway must route `/api/*` to AKS, `/web/*` to App Service.

**Answer:**
Create two backend pools, set path-based routing rules, and use health probes for each. Attach WAF policy scoped per listener.
**Sample Points:**

- Path-based routing separates backends.
- WAF scoped per route for granularity.
- Health probes match backend expectations.
  **Example Code:**

```
az network application-gateway url-path-map create --gateway-name
myagw --resource-group rg ...
```

---

## Q11: Azure Storage SAS token leaked.

**Answer:**
Revoke the SAS by regenerating the account key (if account SAS) or deleting the stored access policy (if service SAS with policy). Rotate keys in dependent apps.
**Sample Points:**

- Account key regen invalidates SAS.
- Delete stored access policy to revoke.
- Rotate creds in apps immediately.

**Example Code:**

```
az storage account keys renew --account-name mystorage --key primary
```

---

## Q12: Azure Service Bus queue messages are delayed; active message count high.

**Answer:**
Scale consumers, enable **prefetch** in clients, and consider partitioned queues for higher throughput. Monitor with Azure Monitor metrics.
**Sample Points:**

- Prefetch reduces round-trips.
- Partitioned queues increase scale.
- `Monitor ActiveMessageCount.`

**Example Code:**

```
az servicebus queue update --name myqueue --enable-partitioning true
```

---

## Q13: AKS nodepool upgrade fails due to insufficient PodDisruptionBudget allowances.

**Answer:**
Adjust PDBs to allow at least one pod eviction at a time or temporarily remove PDBs for upgrade. Use maxUnavailable in upgrade strategy.

**Sample Points:**

- PDBs block upgrades if too strict.
- Temporary relax during maintenance.
- Adjust maxUnavailable in nodepool.
  **Example Code:**

```
az aks nodepool upgrade --cluster-name myaks --name np1
--max-unavailable 1
```

---

## Q14: Azure Key Vault secret rotation fails for a VM app using SDK.

**Answer:**
Ensure the app fetches secrets at runtime instead of caching indefinitely. Use Key Vault event grid notifications to trigger config reload or VM extension script.

**Sample Points:**

- Runtime secret fetch avoids stale values.
- Event Grid triggers reload logic.
- Monitor secret version in app telemetry.
  **Example Code:**

```
az eventgrid event-subscription create --source-resource-id $(az
keyvault show --name kv --query id -o tsv) ...
```

---

## Q15: Azure Monitor alert rules fail to trigger for custom metrics.

**Answer:**
Custom metrics must be sent to the correct namespace and resource ID. Ensure metric ingestion latency is considered in alert eval period.
**Sample Points:**

- Correct metric namespace.
- Align alert period with metric frequency.
- Check ingestion latency.
  **Example Code:**

```
az monitor metrics alert create --name highcpu --resource myvm
--condition "avg Percentage CPU > 80"
```

---

## Q16: VNet Peering between prod and dev doesn’t allow DNS resolution.

**Answer:**
Enable **Allowforwardedtraffic** and **Use remote gateways** in peering config, and link both VNets to the same Private DNS Zone.
**SamplePoints:**

- Peering settings for routing.
- Private DNS zone link required.
- No overlapping CIDRs.
  **Example Code:**

```
az network private-dns link-vnet create --zone-name priv.local
--vnet-name prod-vnet ...
```

---

## Q17: Azure Policy remediation task stuck in “Pending” state.

**Answer:**
Policy assignment might lack `Microsoft.Authorization/policyAssignments/write` or remediation task identity lacks resource write permissions. Assign `Contributor to` remediation identity.

**Sample Points:**

- Remediation identity needs write perms.
- Check policy effects (`DeployIfNotExists`).
- Ensure resource provider registered.

**Example Code:**

```
az role assignment create --assignee <remediationMSI> --role
Contributor --scope /subscriptions/xxx
```

---

## Q18: Azure App Gateway WAF blocks valid requests due to false positives.

**Answer:**
Enable detection mode to log without blocking, exclude specific rules using custom WAF rules, then re-enable prevention mode.

**Sample Points:**

- Detection mode for testing.
- Rule exclusions for false positives.
- Re-enable prevention after tuning.

**Example Code:**

```
az network application-gateway waf-policy custom-rule create
--policy-name mywaf ...
```

---

## Q19: Azure Backup job fails for VM in a zone-redundant storage account.

**Answer:**
Zone-redundant accounts aren't supported for some backup scenarios. Move backup vault to same region/storage type, or reconfigure VM's storage to LRS/GRS as supported.
**Sample Points:**

- Match vault and storage account types.
- Some features exclude ZRS.
- Plan region/storage at design time.
  **Example Code:**

```
az backup protection disable --item-name myvm --vault-name myvault
```

---

## Q20: App Service scaling events are slow to react to traffic surges.

**Answer:**
Switch from scheduled/CPU rules to **HTTP queue length** or custom metric scaling. Enable scale-out cooldown to 0 for rapid growth.
**Sample Points:**

- Scale on queue/throughput metrics.
- Remove cooldown for bursts.
- Balance cost vs scale speed.
  **Example Code:**

```
az monitor autoscale rule create --resource myapp --condition
"Requests > 100" ...
```

---

## Q21: ExpressRoute traffic to Azure SQL is failing.

**Answer:**
Ensure route filters include Microsoft SQL service, and Azure SQL firewall allows your on-prem IP ranges. Verify BGP session health.
**Sample Points:**

- Route filter includes needed service.
- SQL firewall updated for on-prem ranges.
- Check BGP peering state.
  **Example Code:**

```
az network express-route list-route-tables --name myer --peering-name
AzurePrivatePeering
```

---

## Q22: Azure DevOps pipeline needs to deploy to AKS without storing kubeconfig.

**Answer:**
Use `az aks get-credentials --admin --overwrite-existing` in pipeline with SP/MSI auth, or use Azure DevOps AKS service connection.
**Sample Points:**

- Service connection avoids kubeconfig storage.
- SP/MSI with RBAC roles.
- Ephemeral kubeconfig per job.
  **Example Code:**

```
az aks get-credentials --name myaks --resource-group rg
--overwrite-existing
```

---

## Q23: NSG rule changes don’t apply immediately to VM traffic.

**Answer:**
Check if rules applied at subnet vs NIC level; conflicts cause precedence issues. Ensure no effective deny from higher-precedence rule.
**Sample Points:**

- Subnet vs NIC NSG precedence.
- Use “Effective security rules” view.
- Resolve conflicts.
  **Example Code:**

```
az network nic list-effective-nsg --name mynic --resource-group rg
```

---

## Q24: Azure Firewall policy must allow only approved FQDNs for egress.

**Answer:**
Use application rules with target FQDNs, enable DNS proxy, and block all else with default deny.
**Sample Points:**

- App rules filter on FQDN.
- DNS proxy for name resolution.
- Default deny is last rule.
  **Example Code:**

```
az network firewall application-rule create --collection-name
allow-web ...
```

---

## Q25: Azure Files must be mounted to AKS with AD-based auth.

**Answer:**

Enable Azure AD Kerberos integration for Azure Files, create storage account with `Azure AD Kerberos` enabled, and mount using csi-driver SMB with proper secrets.

**Sample Points:**

- Azure AD Kerberosfor Files.
- CSI SMB driverinAKS.
- Secrets store forcredentials.

**Example Code:**

```
kubectl apply -f azurefile-csi.yaml
```