PREPKLOUD FIELD GUIDE SERIES

Azure Administrator AZ-104 Field Guide

A hands-on, scenario-first guide to managing Azure identity, storage, compute, networking, and operations.

First edition · 2026 · prepkloud.com

About this guide

AZ-104 is for Azure administrators who implement, manage, and monitor environments—not just name cloud services. This guide follows the Microsoft Learn skills outline effective April 17, 2026: identity and governance (20–25%), storage (15–20%), compute (20–25%), virtual networking (15–20%), and monitoring and maintenance (10–15%). The official scope includes the portal, PowerShell, Azure CLI, ARM/Bicep, and Microsoft Entra ID.

Each chapter gives you a decision rule, a realistic scenario, and a validation question. Attempt the questions in Chapter 12 before reading the explanations. Use the optional lab in Chapter 11 only in a disposable subscription with a budget, synthetic data, and a cleanup plan; it can incur costs.

Independent publication: Microsoft, Azure, Microsoft Entra, and AZ-104 are Microsoft trademarks. PrepKloud is not affiliated with Microsoft. Service behavior, limits, and exam objectives can change. Recheck the official AZ-104 study guide before your exam. All questions below are original, not exam dumps or recalled items.

Contents

How to prepare for AZ-104

Unlike a fundamentals exam, AZ-104 asks what an administrator would configure, verify, and troubleshoot. A question may supply an existing environment and demand the *smallest* change that satisfies an access, availability, or recovery constraint. Read the existing state first; then identify the exact resource scope, traffic path, and control plane involved.

Current skills domain	Weight	Study chapters
Manage Azure identities and governance	20–25%	2–3
Implement and manage storage	15–20%	4–5
Deploy and manage Azure compute resources	20–25%	6–7
Implement and manage virtual networking	15–20%	8–9
Monitor and maintain Azure resources	10–15%	10

1. **Find the scope:** tenant, management group, subscription, resource group, resource, VNet, subnet, or NIC.
2. **Identify the layer:** identity, data access, network access, availability, or observability.
3. **Check the constraint:** minimum privilege, no public exposure, availability-zone failure, cheapest supported design,

or least downtime.

4. **Validate:** how would you prove it works—effective permissions, network diagnostics, metrics, backup restore, or deployment output?

> **Exam trap**
>
> Contributor at a resource group can manage resources, but cannot grant role assignments merely by being Contributor. A Reader role allows viewing, not modifying. A resource lock prevents management-plane operations; it is not a substitute for data access controls.

Recall

- Can I name the five current domains?
- Can I identify the control plane and scope before picking an Azure feature?

Microsoft Entra users, groups, and access

Microsoft Entra ID holds identities that authenticate to Azure and connected applications. Azure RBAC then authorizes management of Azure resources; those are separate decisions. A user may exist in Entra and still have no access to a subscription. For large teams, assign access to groups rather than maintaining a separate role assignment for every person.

Administrative task	What to check
Onboard a team	Create/maintain a group, assign the group an appropriate role at the narrowest practical scope.
Invite an external collaborator	Use an external user/guest invitation and a limited access assignment; review lifecycle.
User forgot password	Self-service password reset requires configuration and applicable licensing/policy.
Person has a license but no resource access	License assignment does not grant Azure RBAC access.

Groups simplify changes in membership; role assignments remain scoped. Different identity types also have different purposes: a managed identity is a service identity used by Azure workloads to request tokens without hardcoded credentials. It is not a human

user's password. Use least privilege for both humans and workloads.

> **Contractor's audit**
>
> A contractor needs to inspect resources in one resource group but should change nothing. Invite an external user, then assign Reader at that resource group. Contributor at subscription scope violates both the minimum privilege and the requested boundary.

Recall

- Can I separate identity authentication from Azure resource authorization?
- Can I choose a group and resource-group scope instead of repetitive broad assignments?

Azure RBAC, subscriptions, and governance

Azure's management hierarchy is management group → subscription → resource group → resource. An Azure RBAC assignment at a parent scope applies to its children. Built-in roles include Reader (view), Contributor (manage resources but not role assignments), and Owner (manage resources and access). Compare allowed actions and scope together; a narrowly scoped Owner is not the same as subscription-wide Reader.

Requirement	Choose or inspect
Enforce configuration rule across subscriptions	Azure Policy at management group or subscription scope.
Prevent accidental deletion or modification	Delete or ReadOnly resource lock as appropriate.
Identify spend by department	Tags plus cost analysis and budgets.
Group subscriptions for centralized policy	Management groups.
See improvement recommendations	Azure Advisor.

Azure Policy evaluates whether resources meet rules and may deny noncompliant deployments, audit, or remediate depending on the definition/effect. RBAC answers *who may perform actions*;

Policy answers *which resource configurations are permitted*. Locks restrict control-plane changes but do not replace RBAC or protect against every data-plane deletion. Tags organize and allocate costs but do not inherently change security or availability.

> **Region restrictions**
>
> An organization requires every new resource in an approved Region. Apply a location policy at the appropriate parent scope, then test a nonapproved deployment. A tag named "approved" would report intent but would not enforce a Region restriction.

Recall

- Can I list the scope hierarchy and explain inheritance?
- Can I distinguish Policy, RBAC, lock, tag, budget, and Advisor?

Storage security and redundancy

A storage account controls namespace, region, redundancy, and many access settings. Different controls address different threats: encryption protects stored data, TLS protects traffic, identity-based access limits who may access, and firewall/private networking limits the network path. The administrator chooses the combination specified by the scenario.

Redundancy	Protection goal	Tradeoff
LRS	Copies within a single datacenter/location in a Region.	Low cost; not a zone or regional DR design.
ZRS	Synchronous copies across zones in a Region.	Zone resilience where available.
GRS	Copies to a secondary Region, with asynchronous geo-replication.	Potential lag; secondary-read access requires an appropriate read-access option.
GZRS	Zone resilience in primary Region plus geo-replication.	More coverage with higher cost/availability constraints.

Azure Storage firewalls can restrict networks; private endpoints give a private IP in a VNet for a storage service. Service endpoints let a subnet identify itself to supported Azure services while the service still uses its public endpoint; do not confuse the two. A **shared access signature (SAS)** delegates scoped, time-limited

access; reduce its permissions and lifetime. Account keys grant broad access and require careful rotation. Stored access policies can help control certain service-level SAS tokens.

> **Bank's document store**
>
> The company requires no public network route and access limited to its VNet. Configure a private endpoint and appropriate name resolution plus storage public access restrictions. Turning on encryption alone does not remove the public network path.

Recall

- Can I choose LRS vs ZRS vs GRS vs GZRS based on failure scope?
- Can I distinguish SAS, account key, identity-based access, firewall, and private endpoint?

Blobs, files, lifecycle, and recovery

Azure Blob Storage holds unstructured objects; Azure Files exposes managed file shares using supported file protocols. Blob containers organize objects inside a storage account. For file shares, consider identity-based access and share permissions. For blobs, choose access tiers based on retrieval pattern: Hot for frequent use, cooler online tiers for infrequent access, Archive for offline data that tolerates rehydration.

Feature	Use it when…
Blob soft delete	Recover deleted blobs during the configured retention period.
Container soft delete	Recover a deleted container (distinct from blob-level protection).
Blob versioning	Recover earlier versions after overwrite or change.
Blob lifecycle management	Automatically transition or expire objects/versions according to rules.
Azure Files snapshots	Retain point-in-time copies of file shares.
Object replication	Asynchronously replicate eligible blob data according to a policy.

Azure Storage Explorer provides a graphical client for storage operations; **AzCopy** is useful for scripted/high-volume transfers. Neither changes redundancy or access policy automatically. A

common exam combination is enabling versioning/soft delete for recovery and lifecycle rules for accumulated old versions' cost.

> **Accidental overwrites**
>
> A team edits frequently accessed customer files and needs prior contents after accidental overwrites. Blob versioning directly addresses overwritten content. Selecting GRS alone replicates changes and is not a substitute for version history.

Recall

- Can I distinguish deleted-object recovery from cross-region redundancy?
- Can I explain lifecycle, versioning, snapshots, and the access tiers?

ARM/Bicep, VMs, and scale sets

Azure Resource Manager (ARM) evaluates declarative deployments. JSON ARM templates and Bicep express resources, parameters, dependencies, and outputs. Bicep provides a concise language that deploys through ARM. For repeatable infrastructure, parameterize environment-specific values and review changes before deployment; an exported template may still need cleanup before reuse.

Virtual machines provide OS-level control. Pick a size for CPU/memory/workload, attach suitable managed disks, and plan access and backup. Deploy instances across **availability zones** for zone-failure protection where supported; **availability sets** distribute instances across fault and update domains within a datacenter context. Azure Virtual Machine Scale Sets manage a group of VMs and support scaling; a single manually resized VM is not equivalent to horizontal autoscaling.

Change	Operational question
Resize VM	Will size be available in this region/zone, and is deallocation required?
Move VM/resource	Does this resource type support the target scope/region and its dependencies?
Encryption at host	Is host-side disk encryption required and supported for the VM?

VM Scale Sets	What signal drives scaling and how are instances managed?

> **Consistent staging environments**
>
> A team repeatedly creates nearly identical VM/network stacks. A parameterized Bicep/ARM deployment provides consistency; clicking through each environment by hand risks drift. Use deployment outputs to verify created resource IDs and endpoints.

Recall

- Can I explain ARM/Bicep and parameters/outputs?
- Can I distinguish availability zone, availability set, and VM Scale Set?

App Service and containers

Azure App Service hosts web applications with managed platform operations. An **App Service plan** defines compute capacity and certain features; an **App Service app** hosts code. Scaling out adds instances; scaling up changes the plan's capacity/tier. Deployment slots let you validate a release before swapping traffic, subject to slot behavior and supported tiers. TLS certificates and custom domains must match the application endpoint configuration.

Azure Container Registry (ACR) stores container images. **Azure Container Instances (ACI)** runs containers without an orchestration platform for suitable simple/burst workloads. **Azure Container Apps** runs managed containerized applications with app-level features and scaling. The exam expects you to provision/manage containers and recognize which service fits the operational need; it does not require designing a full Kubernetes platform.

Requirement	Likely fit
Managed web app with staging/release slots	App Service with an appropriate plan tier.
Private image repository for deployed apps	Azure Container Registry.
Run a straightforward container without orchestrating clusters	Azure Container Instances.

Managed containerized app that needs scaling and revisions	Azure Container Apps.

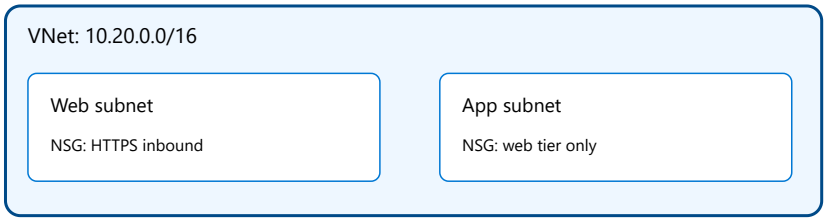
> **Deployment distinction**
>
> An image registry stores images; it does not run them. Selecting ACR without a compute service does not meet "run this container" requirements. Similarly, changing the App Service plan can affect other apps sharing the plan.

Recall

- Can I distinguish a plan from an App Service app and describe scale-out vs scale-up?
- Can I choose between ACR, ACI, and Container Apps?

VNets, routes, NSGs, and private access

Azure Virtual Networks (VNets) define address spaces and contain subnets. Plan nonoverlapping ranges before peering or connecting on premises. A user-defined route influences where traffic goes; a network security group (NSG) governs allowed/denied traffic through rules. Application security groups (ASGs) help reference workloads in NSG rules without managing each IP individually.



Subnet-level network segmentation; routes determine paths, NSGs filter traffic.

NSGs are stateful; rules are evaluated by priority (lower numeric value wins), and effective security rules combine applicable subnet and NIC rules. VNet peering connects two VNets; check address-space overlap and gateway/traffic settings. **Service endpoints** provide VNet identity to supported PaaS services while using the service's public endpoint. **Private endpoints** give a private IP in your VNet for a specific service instance and often require private

DNS configuration. **Azure Bastion** enables administrative RDP/SSH access to VMs without exposing public IPs on the VMs.

> **VM access without public IPs**
>
> Admins must manage VMs by RDP/SSH, but VMs must not expose public IPs. Deploy and authorize Azure Bastion, and verify routing/NSG access. Exposing RDP from the whole internet contradicts the requirement.

Recall

- Can I distinguish routing from filtering?
- Can I explain service vs private endpoints and the role of DNS?
- Can I troubleshoot effective NSG rules?

DNS, load balancing, and troubleshooting

Azure DNS hosts DNS zones/records to resolve names; public and private resolution have different scopes. A private endpoint that resolves to a public address can fail an otherwise correct "private-only" design, so DNS is part of connectivity validation. Azure Load Balancer distributes transport-layer traffic to healthy backend instances. Choose a public frontend for internet clients or an internal frontend for private consumers, and verify health probes before blaming application instances.

Symptom	Check first
VM cannot connect to a target	Effective NSG rules, effective routes, address resolution, target health.
Load balancer has no healthy backends	Probe protocol/port, app listener, NSG path.
Private endpoint still resolves publicly	Private DNS zone linking and record resolution.
Two VNets cannot peer	Overlapping address spaces and peering configuration.

Azure Network Watcher and Connection Monitor provide tools to investigate connectivity. A metric showing traffic dropped is a symptom; the root cause can be an NSG deny, a route to the wrong next hop, a closed application port, or DNS pointing

somewhere unexpected. Work through the path in order rather than opening broad firewall rules.

Recall

- Can I distinguish DNS resolution, routing, filtering, and load-balancer health?
- Can I explain an internal vs public load balancer?

Monitor, backup, and disaster recovery

Azure Monitor collects metrics and logs; Azure Monitor Logs in a Log Analytics workspace support Kusto Query Language (KQL) queries. Metric alerts react to numerical measurements; log search alerts use query results. An **action group** defines what happens when an alert fires; an alert processing rule adjusts how alerts are handled. Azure Monitor Insights provides prebuilt views for supported resources.

Azure Backup protects supported workloads using vaults and backup policies. A policy defines frequency/retention; a successful backup is not proof that a restore meets business recovery objectives, so validate a restore in a safe environment. **Azure Site Recovery** orchestrates replication and failover for disaster recovery. Backup retention and regional failover are not the same problem.

Business requirement	Primary direction
Alert if VM CPU exceeds a threshold	Azure Monitor metric alert + action group.
Analyze application logs for repeated failures	Log Analytics query and a log-based alert if needed.
Restore an earlier VM state	Azure Backup, policy/vault, tested restore.

Fail over workloads to another region	Azure Site Recovery, replication, failover plan.
Identify a network connectivity problem	Network Watcher/Connection Monitor plus effective rules and routes.

> **Recovery terms**
>
> RPO is the acceptable period of lost data; RTO is the acceptable time to restore service. “Daily backup” cannot by itself satisfy a five-minute RPO. Define the target before selecting protection.

Recall

- Can I distinguish metric vs log alerts and the action group?
- Can I choose backup vs Site Recovery?
- Have I tested recovery rather than merely configuring it?

Safe administrator lab

This lab turns the five domains into one small evidence package. It is optional and may incur Azure charges. Use a disposable subscription, synthetic data, narrow permissions, and a budget/alert. Azure budgets alert but do not guarantee a hard spending limit. Do not use a work account or production subscription without authorization.

1. Write a one-page scope: two test users/groups, one resource group, one VNet and subnet, one storage account with private access settings, and a cleanup checklist. Estimate costs before creating anything.
2. Assign Reader to a test group at the resource-group scope; verify it can view resources but cannot change them. Remove the assignment afterward.
3. Define a storage account configuration with appropriate redundancy and soft delete/versioning using ARM/Bicep or the portal. Upload only a harmless synthetic file; verify access controls and recovery behavior.
4. Sketch a VNet path from client to storage. If creating a private endpoint, verify DNS resolves to a private IP and review endpoint billing. Avoid unnecessary VMs or always-on resources.
5. Create a test metric alert/action group on a supported resource; inspect whether the alert and action group are

separate configurations.

6. Delete created resources and test identities/assignments, check for dependent resources in other resource groups, then verify actual spend after billing data settles.

> **Portfolio evidence**
>
> Keep an architecture diagram, redacted screenshots of effective permissions and networking, deployment notes, one test outcome (including a failed unauthorized action), a cost estimate, and proof of cleanup. Explain *why* each setting was chosen, not just where you clicked.

Practice questions and explanations

Answer from the stated constraint. These items are original scenarios, not recalled certification questions.

Identity and governance (1–7)

1. A guest auditor needs read-only access to one resource group. What is the narrowest common built-in assignment?

Reader at the resource-group scope.
Subscription scope is broader; Contributor would allow changes.

2. An administrator can manage VMs but cannot grant another person an Azure RBAC role. Which built-in role likely describes this?

Contributor.
It manages resources but lacks access-management permission by default.

3. Every new resource across three subscriptions must be in approved regions. Which control should enforce this?

Azure Policy at a management-group or other common parent scope.

Tags report metadata; they do not enforce placement.

4. A project lead wants a warning at a defined monthly spending threshold. Which Azure feature?

A cost-management budget and alert.

Budgets notify; do not assume a universal hard spending shutoff.

5. A workload needs Azure credentials without a password stored in configuration. What identity type fits?

A managed identity with an appropriate scoped role.

Its token-based access avoids embedded long-lived credentials.

6. A resource-group lock prevents accidental deletion. Does it replace blob-level data permissions?

No.

Locks primarily protect management-plane operations; data access requires separate controls.

7. A user exists in Microsoft Entra ID but cannot view a subscription. What should be checked?

An Azure RBAC assignment at an applicable scope.
Being an identity in the tenant does not grant subscription access.

Storage (8–13)

8. A service must remain available after an Availability Zone failure inside its Region. Which storage redundancy should be considered?

ZRS (or GZRS if geo-replication is also required).
LRS does not provide zone-level distribution.

9. Users sometimes overwrite a blob and need earlier versions. Which feature directly addresses this?

Blob versioning.
Geo-redundancy replicates data but does not provide version history.

10. A contractor may upload to a container for one day without receiving an account key. What should be issued?

A narrowly scoped, short-lived SAS.
Account keys give overly broad control for a temporary task.

11. An application may access its storage account only via a private IP in a VNet. Which feature?

A private endpoint with corresponding private DNS.
Service endpoints do not assign a private IP for that storage resource.

12. Historical blobs should move to a cheaper tier after a set age. Which setting automates this?

Blob lifecycle management.
Changing account redundancy does not tier blobs by age.

13. A team needs an SMB-style managed file share rather than object storage. Which Azure storage service?

Azure Files.
Blob Storage is object-based, not a general shared file-system replacement.

Compute (14–19)

14. Infrastructure must deploy consistently across test and staging with different address ranges. Which approach?

Parameterize an ARM/Bicep template.

It makes repeatable deployments with environment-specific inputs.

15. VM application capacity should automatically grow with increased demand. Which Azure resource?

Azure Virtual Machine Scale Sets.

Manually resizing one VM is not horizontal autoscaling.

16. A web app release must be tested at a staging endpoint before swapping to production. Which feature?

App Service deployment slots on a supporting tier.

Slots separate staged deployment from the live endpoint.

17. A team needs to store private container images but not run containers yet. Which service?

Azure Container Registry.

ACI/Container Apps run workloads; ACR stores images.

18. A team needs to run a straightforward container without managing a cluster. Which option fits?

Azure Container Instances.

ACR alone does not execute the container.

19. A web app needs more parallel instances without changing instance size. Which scaling operation?

Scale out the App Service plan.

Scale up changes plan tier/instance capacity.

Networking (20–25)

20. Which network control explicitly allows or denies traffic to a subnet or NIC?

A network security group (NSG).

A route changes the next hop, not whether the packet is permitted.

21. An administrator needs RDP to a VM with no public IP on the VM. Which Azure service helps?

Azure Bastion.

It provides browser-based secure administrative connectivity via the VNet.

22. Two VNets must connect but use the same overlapping address range. What is the blocker?

Overlapping address spaces prevent normal VNet peering.
Plan nonoverlapping ranges before establishing peering.

23. A service's private endpoint resolves to a public IP from a VM. What should be checked?

Private DNS configuration and VNet links.
A private endpoint needs correct name resolution for clients to use its private IP.

24. Load balancer traffic reaches no backend even though VMs run. Which configuration should be inspected?

The backend health probe, app listener, and NSG path.
Running VMs do not automatically count as healthy targets.

25. A custom route sends VM traffic to the wrong next hop. Where should the administrator look?

Effective routes and the user-defined route table.
Changing DNS will not correct an incorrect network route.

Monitoring and recovery (26–30)

26. An operator wants email when VM CPU rises above a threshold. What two components are needed?

A metric alert rule and an action group.
The alert defines when; the action group defines notification.

27. A team wants to query stored VM diagnostic events with KQL. Which platform?

Azure Monitor Logs in a Log Analytics workspace.
Numeric metric charts alone cannot replace log queries.

28. A company needs yesterday's VM state restored. Which service?

Azure Backup with an appropriate policy and recovery point.
Site Recovery addresses failover rather than restoring an older backup state.

29. Workloads must be orchestrated to fail over to another Azure Region. Which service?

Azure Site Recovery.
A backup vault alone is not a region failover orchestration plan.

30. Backups run once a day but the business tolerates only five minutes of data loss. Does the design meet the RPO?

No.

RPO is acceptable lost data in time; daily recovery points do not guarantee a five-minute RPO.

Six-week plan, quick reference, and glossary

Week	Primary focus	Evidence to collect
1	Entra identities and Azure RBAC	Explain scope inheritance and least privilege.
2	Policy, tags, locks, budgets, storage security	Match controls to four governance scenarios.
3	Blob/File protection, redundancy, lifecycle	Compare storage recovery requirements.
4	ARM/Bicep, VMs, VMSS, App Service, containers	Choose compute from operational constraints.
5	VNet, peering, NSGs, routes, endpoints, DNS	Trace client-to-service traffic and identify blockers.
6	Monitor, backup, Site Recovery, mixed review	Attempt timed questions and explain every miss.

Decision cheat sheet

- **RBAC / Policy / lock:** who can act / what configurations are allowed / what management changes are blocked.
- **Managed identity / SAS / account key:** workload identity / delegated limited access / broadly scoped secret.
- **LRS / ZRS / GRS / GZRS:** local / zone / geo / zone plus geo.

- **Private endpoint / service endpoint:** private IP for service instance / VNet identity using service public endpoint.
- **NSG / route / DNS:** filter traffic / choose path / resolve destination.
- **Backup / Site Recovery:** restore point / failover workflow.

Glossary

Action group
Notifications and actions triggered by an alert.

Azure RBAC
Role assignments granting actions at an Azure resource scope.

Bicep
Declarative language for Azure Resource Manager deployments.

Blob versioning
Preservation of previous blob versions after changes.

Managed identity
Azure-managed workload identity for token-based access.

Network security group (NSG)
Stateful rules filtering network traffic.

Private endpoint
Private IP in a VNet for access to a particular service instance.

RPO
Maximum acceptable data loss in time.

RTO

Maximum acceptable time to restore service.

Scale set
Managed group of VMs that can scale and be maintained together.

Before test day, compare this book with Microsoft's current study guide, practice one safe restore or connectivity diagnosis, and avoid memorizing short-lived pricing or platform limits. The best answer satisfies the stated requirement at the correct scope.