Azure Estate Report

Quarterly estate review

Contoso Ltd

Tenant `fixture-tenant` · Snapshot `dced93ea-6655-418a-ac15-a87608cee6ab`
Collected 2026-09-15T17:34:04.175996+00:00 · Status complete

Contents

Executive assessment

The collected estate contains 18 resources in 2 subscriptions. Its 13 finding occurrences come from 5 recurring checks and refer to 11 distinct resource IDs. Review the recurring configuration patterns and their concentrations before assigning work to individual resources.

18	5	11
Resources	Recurring checks	Affected resources

Principal observations

UK South holds 15 resources, 83% of the inventory. This describes resource placement; it does not establish workload failover, data residency compliance or recovery capability.

Production contains the largest resource population: 15 resources, 83% of the estate. Resource counts include supporting infrastructure and are not a measure of spend or business criticality.

9 resources carry at least one tag and 9 carry none (50% with any tag). Establish the required ownership and classification tags before interpreting this as governance quality.

Decisions to make first

Internet-sourced network security rules: 1 recorded occurrences refer to 1 distinct resource IDs across 1 resolved subscriptions. Verify internet-sourced NSG rules

Internet-sourced network security rules

Storage anonymous-access permission: 1 recorded occurrences refer to 1 distinct resource IDs across 1 resolved subscriptions. Verify storage anonymous-access requirements

Storage anonymous-access permission

Web applications allowing HTTP: 1 recorded occurrences refer to 1 distinct resource IDs across 1 resolved subscriptions. Verify application HTTPS enforcement

Web applications allowing HTTP

The optional technical reference contains key settings for every resource, grouped findings and collection coverage. Use the snapshot database and data exports for the underlying evidence.

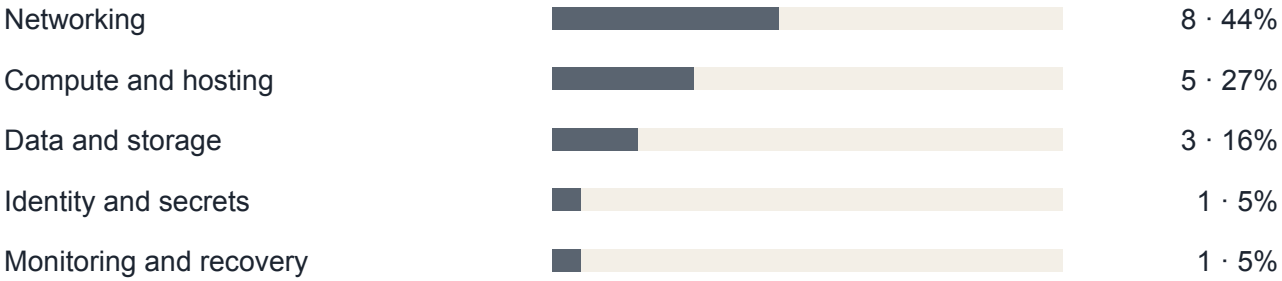
Estate composition

The comparisons below show where the estate is concentrated. Service families describe Azure resource types, including supporting components; application ownership and business purpose are not inferred from naming conventions.

Subscription comparison

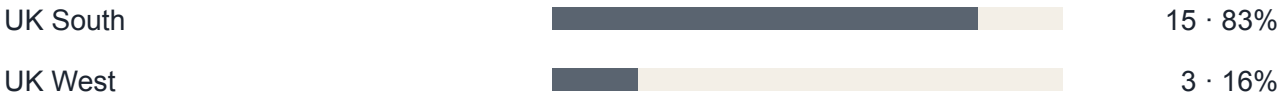
Subscription	Resources	Resource groups	Affected resources
Development	3	1	3
Production	15	2	8

Service composition



Share of recorded resources by service family. Counts include supporting infrastructure and do not measure cost or business importance.

Regional concentration



Global and unrecorded locations remain separate. A region with few resources may still contain an important service; use the subscription profiles and dependencies to interpret the distribution.

Architecture and dependencies

The connections below are extracted from stored resource properties. Direction identifies which resource uses or attaches to another. Containment is excluded from connection counts, and reciprocal VNet peering records count as one connection. These are configuration relationships, not measured traffic flows.

10 distinct non-containment connections are recorded; 1 cross resource-group boundaries. 0 connections have at least one endpoint without a matching resource row. Missing endpoints remain explicit and do not imply a broken service.

Connection patterns

Relationship	Recorded connections
attached to	5
nsg attached	1
peered with	1
private endpoint for	1
runs on	1
uses identity	1

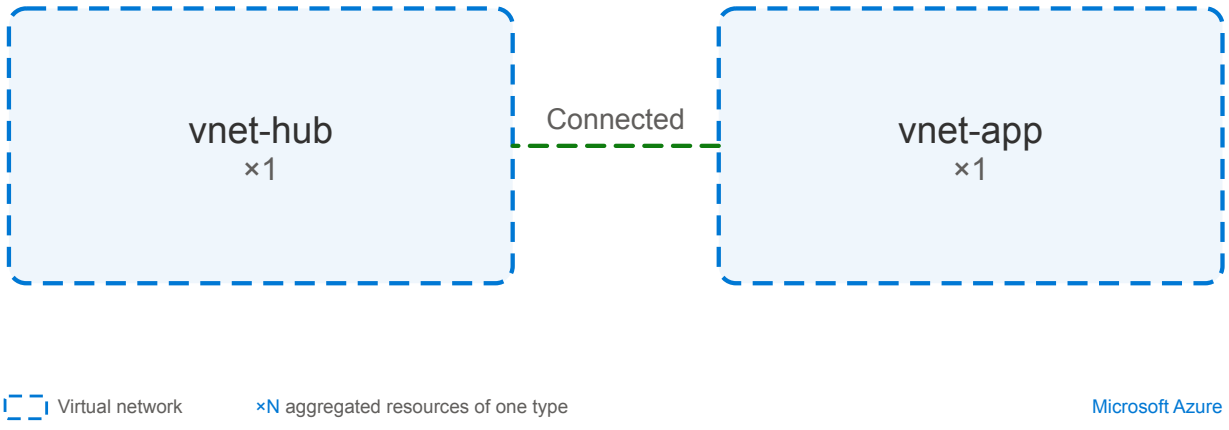
Shared dependencies

These targets have consumers in more than one resource group. Review their ownership, access and change coordination before modifying them. The count describes recorded consumers, not runtime usage or the impact of an outage.

None recorded

Network boundaries

Peering and private endpoints explain configured connectivity. A private endpoint does not by itself establish that a service has disabled public access, or that DNS and client routing use the private path.



Virtual-network peerings recorded in this snapshot. Reciprocal records are shown once; lines describe configuration, not traffic or reachability.

Source	Target
vnet-app	vnet-hub

Private endpoints

Source	Target
pe-sql	sql-prod

Subscription profiles

Each subscription is described through its resource population, regional distribution and recorded findings. Resource-group studies are selected for finding concentration, cross-group connections and population; the technical reference contains the remaining groups and every resource. Figures illustrate up to two connection types per study, prioritising cross-group links and then connection count. Every link of a selected type is retained, with larger figures split across pages.

Development

3 resources in 1 populated resource groups; 0 resources carry at least one tag. 4 finding occurrences affect 3 distinct resources. 0 connections cross this subscription's resource-group boundaries.

rg-dev is the largest populated group with 3 resources (100% of this subscription). Its size includes attached and child resources; the study below describes the service configuration behind that count.

Service composition

Share of recorded resources by service family. Counts include supporting infrastructure and do not measure cost or business importance.

Region	Resources
UK West	3

Largest resource groups

Resource group	Resources	Occurrences	Recorded connections
rg-dev	3	4	0

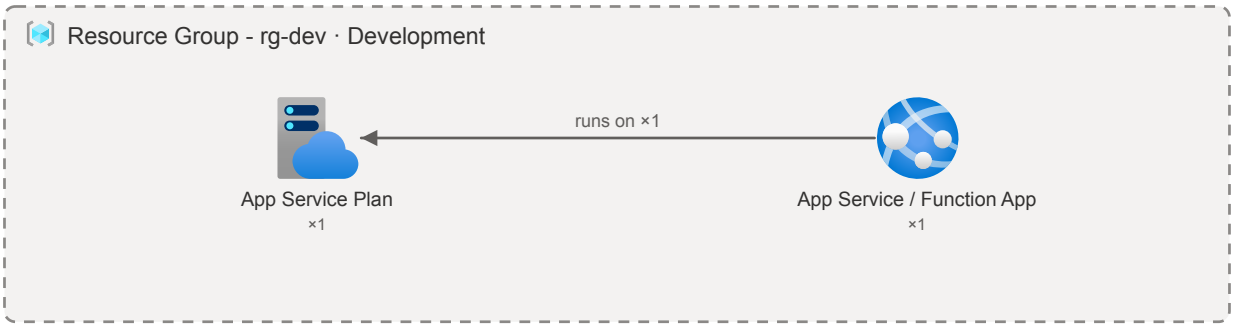
rg-dev

Selected for the highest remaining concentration of recorded finding severity, with high-priority occurrences considered first.

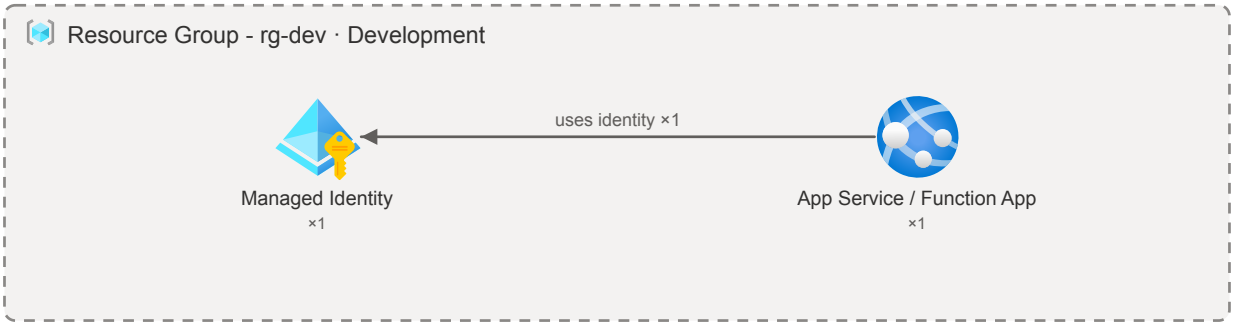
This group contains 3 resources across 3 Azure types, with 4 finding occurrences and 0 connections across its boundary. 0 resources have at least one tag.

App Service / Function App is the largest recorded service type, with 1 of the group’s 3 resources. The composition below includes supporting and child resources; review the settings and connections to distinguish the services from their attachments.

Type	Resources
App Service / Function App	1
App Service Plan	1
Managed Identity	1



runs on: App Service Plan (1 recorded links) Recorded service connections for rg-dev. Attached NICs and disks fold into their host where possible; repeated types are aggregated with counts. External endpoints show dependencies outside this group. Lines count observed links, not every member of an aggregate.



uses identity: Managed Identity (1 recorded links) Recorded service connections for rg-dev. Attached NICs and disks fold into their host where possible; repeated types are aggregated with counts. External endpoints show dependencies outside this group. Lines count observed links, not every member of an aggregate.

Configuration comparisons

Values are taken from the stored properties or collected inventory rows. An unrecorded value is unknown, not a default or evidence of a disabled feature.

Identity and logging configuration

Resource	Identity type	Dependency
web-dev	UserAssigned	runs on: asp-dev uses identity: id-web-dev

Dependencies across the group boundary

No cross-group dependencies are recorded. Resource Graph does not capture every application-level connection, so this does not establish isolation.

Observations to follow up

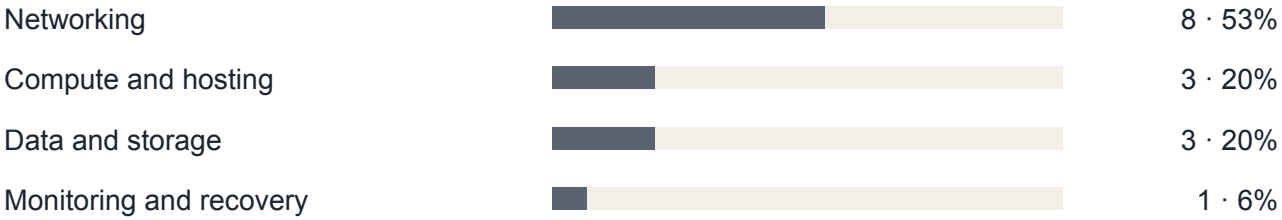
Check	Affected resources
Web applications allowing HTTP	1
Missing required resource tags	3

Production

15 resources in 2 populated resource groups; 9 resources carry at least one tag. 9 finding occurrences affect 8 distinct resources. 1 connections cross this subscription's resource-group boundaries.

rg-app is the largest populated group with 12 resources (80% of this subscription). Its size includes attached and child resources; the study below describes the service configuration behind that count.

Service composition



Share of recorded resources by service family. Counts include supporting infrastructure and do not measure cost or business importance.

Region	Resources
UK South	15

Largest resource groups

Resource group	Resources	Occurrences	Recorded connections
rg-app	12	7	1
rg-network	3	2	1

rg-app

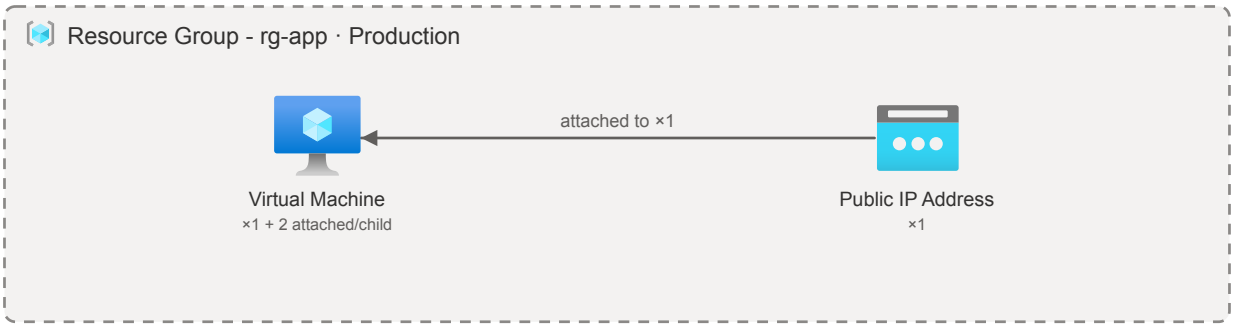
Selected for the highest remaining concentration of recorded finding severity, with high-priority occurrences considered first.

This group contains 12 resources across 11 Azure types, with 7 finding occurrences and 1 connections across its boundary. 6 resources have at least one tag.

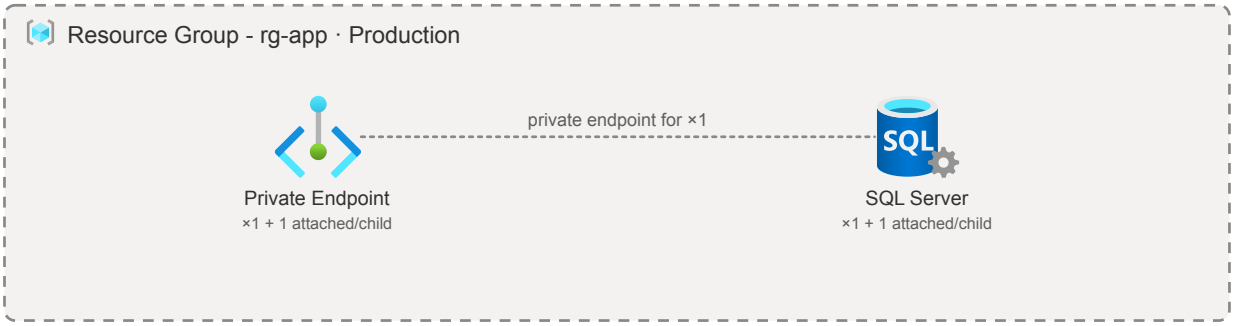
Network Interface is the largest recorded service type, with 2 of the group’s 12 resources. The composition below includes supporting and child resources; review the settings and connections to distinguish the services from their attachments.

Type	Resources
Network Interface	2
AVD Host Pool	1
Log Analytics Workspace	1
Managed Disk	1
Private Endpoint	1
Public IP Address	1

Showing 6 of 11 rows; the snapshot database and data exports retain the underlying evidence.



attached to: Virtual Machine (1 recorded links) Recorded service connections for rg-app. Attached NICs and disks fold into their host where possible; repeated types are aggregated with counts. External endpoints show dependencies outside this group. Lines count observed links, not every member of an aggregate.



private endpoint for: SQL Server (1 recorded links) Recorded service connections for rg-app. Attached NICs and disks fold into their host where possible; repeated types are aggregated with counts. External endpoints show dependencies outside this group. Lines count observed links, not every member of an aggregate.

Configuration comparisons

Values are taken from the stored properties or collected inventory rows. An unrecorded value is unknown, not a default or evidence of a disabled feature.

Compute configuration

Resource	Size or plan	Operating system	Zones
vm-app-01	Standard_B2s	Not recorded	Not recorded

Storage configuration

Resource	SKU or replication	Public network access	Anonymous access permitted
stprodapp01	Not recorded	Not recorded	true

Database network configuration

Resource	Public network access	Default network action
sql-prod	Disabled	Not recorded

Dependencies across the group boundary

0 directed connections enter this group and 0 leave it; 1 peerings cross its boundary. Changes to the named shared targets need coordination with their consumers. These are recorded configuration links, so application dependencies may extend beyond them.

Source	Relationship	Target
vnet-app	peered with	vnet-hub

Observations to follow up

Check	Affected resources
Storage anonymous-access permission	1
Missing required resource tags	6

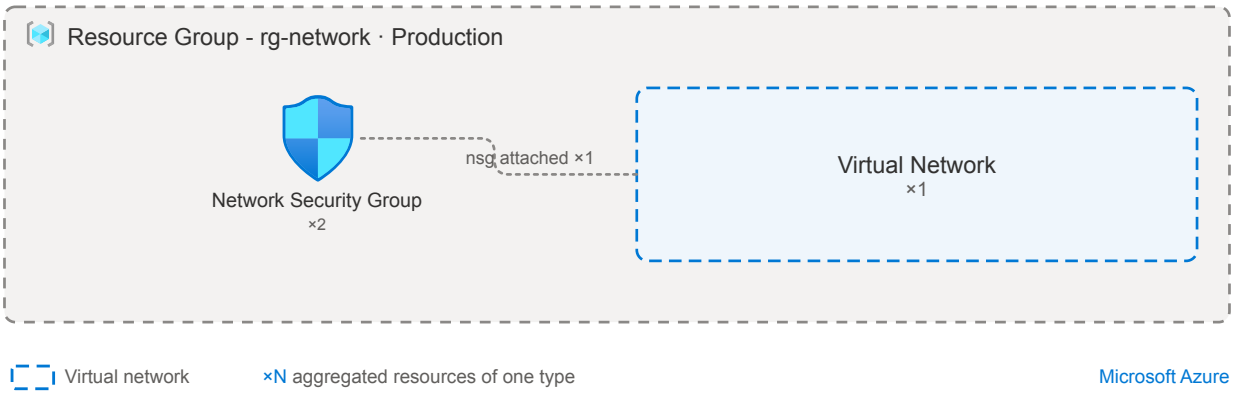
rg-network

Selected for the greatest remaining number of recorded cross-group connections. This highlights dependency coordination rather than assuming business criticality.

This group contains 3 resources across 2 Azure types, with 2 finding occurrences and 1 connections across its boundary. 3 resources have at least one tag.

Network Security Group is the largest recorded service type, with 2 of the group's 3 resources. The composition below includes supporting and child resources; review the settings and connections to distinguish the services from their attachments.

Type	Resources
Network Security Group	2
Virtual Network	1



nsg attached: Network Security Group (1 recorded links) Recorded service connections for rg-network. Attached NICs and disks fold into their host where possible; repeated types are aggregated with counts. External endpoints show dependencies outside this group. Lines count observed links, not every member of an aggregate.

Configuration comparisons

Values are taken from the stored properties or collected inventory rows. An unrecorded value is unknown, not a default or evidence of a disabled feature.

No supported comparison fields are recorded for this group. The technical reference retains its resource details.

Dependencies across the group boundary

0 directed connections enter this group and 0 leave it; 1 peerings cross its boundary. Changes to the named shared targets need coordination with their consumers. These are recorded configuration links, so application dependencies may extend beyond them.

Source	Relationship	Target
vnet-app	peered with	vnet-hub

Observations to follow up

Check	Affected resources
Internet-sourced network security rules	1
Network security groups without an association	1

Audit findings and review priorities

Each recurring check is explained once. Severity labels are retained from collection and describe the audit rule; the assessment distinguishes observed settings, potential exposure and policy choices. Confirm the affected service configuration before making changes.

Internet-sourced network security rules

HIGH Recorded occurrences: 1. Distinct resource IDs: 1. Estate-level occurrences: 0; occurrences without a matching resource row: 0.

Recorded severity mix	Occurrences
High	1

What was observed
The audit recorded network security rules matching the audit's internet-access criteria.

Why it matters
A matching rule may permit internet-sourced traffic, but priority, association, destination and other controls determine the effective path. The stored rule alone does not establish end-to-end reachability.

What to verify
Review rule priority, direction, ports, source ranges and effective rules on associated NICs and subnets.

Policy considerations
Document permitted public entry points and restrict administrative access to approved paths; verify dependencies before changing rules.

Where it is concentrated

Subscription	Affected resources
Production	1

1 affected resources are in rg-network (Production), the largest resolved group concentration for this check.

Evidence examples

- nsg-app: rule allow-ssh allows Internet -> port 22

Showing 1 of 1 occurrences. The technical reference groups all occurrences by resource; original titles and stored evidence remain in the snapshot database and data exports.

Source: the original stored finding and its collection-time query evidence.

Storage anonymous-access permission

HIGH Recorded occurrences: 1. Distinct resource IDs: 1. Estate-level occurrences: 0; occurrences without a matching resource row: 0.

Recorded severity mix	Occurrences
High	1

What was observed
The audit recorded storage accounts with the account-level permission for anonymous blob access enabled.

Why it matters
This permits containers to be configured for anonymous access. It does not establish that any container or blob is currently public; container access level and network controls also matter.

What to verify
Inspect container access levels and known anonymous consumers. Disable the account permission where anonymous delivery is not intended, after validating dependent services.

Policy considerations
Public content delivery may be intentional. Document its scope and separate it from confidential data rather than treating every permitted account as a confirmed disclosure.

Where it is concentrated

Subscription	Affected resources
Production	1

1 affected resources are in rg-app (Production), the largest resolved group concentration for this check.

Evidence examples
- stprodapp01 allows public blob access

Showing 1 of 1 occurrences. The technical reference groups all occurrences by resource; original titles and stored evidence remain in the snapshot database and data exports.

Source https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure

Web applications allowing HTTP

MEDIUM Recorded occurrences: 1. Distinct resource IDs: 1. Estate-level occurrences: 0; occurrences without a matching resource row: 0.

Recorded severity mix	Occurrences
Medium	1

What was observed
The audit recorded web applications that do not enforce HTTPS-only access.

Why it matters
Applications may accept requests over HTTP unless another layer redirects or blocks them. Review the complete ingress path, including proxies and custom domains.

What to verify
Test HTTP and HTTPS behaviour, redirects and dependent clients. Enable HTTPS-only where required after confirming certificates and client compatibility.

Policy considerations
Define transport requirements for public and private application endpoints.

Where it is concentrated

Subscription	Affected resources
Development	1

1 affected resources are in rg-dev (Development), the largest resolved group concentration for this check.

Evidence examples

- web-dev does not enforce HTTPS-only traffic

Showing 1 of 1 occurrences. The technical reference groups all occurrences by resource; original titles and stored evidence remain in the snapshot database and data exports.

Source https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings

Missing required resource tags

> LOW Recorded occurrences: 9. Distinct resource IDs: 9. Estate-level occurrences: 0; occurrences without a matching resource row: 0.

Recorded severity mix	Occurrences
Low	9

What was observed
The audit recorded resources missing at least one tag required by the collection-time audit.

Why it matters
Missing classification keys make ownership and cost allocation harder to establish. A present key may still hold an empty or unsuitable value, so key presence alone does not establish useful classification.

What to verify
Use the stored missing-key evidence to identify owners and correct omissions; do not substitute today's tag policy.

Policy considerations
Use the collection-time missing keys as evidence and confirm the current required keys, accepted values and exception process with their owners.

Where it is concentrated

Subscription	Affected resources
Development	3
Production	6

6 affected resources are in rg-app (Production), the largest resolved group concentration for this check.

Evidence examples
- id-web-dev is missing tags: env
- asp-dev is missing tags: env
- web-dev is missing tags: env

Showing 3 of 9 occurrences. The technical reference groups all occurrences by resource; original titles and stored evidence remain in the snapshot database and data exports.

Source: the original stored finding and its collection-time query evidence.

Network security groups without an association

INFO Recorded occurrences: 1. Distinct resource IDs: 1. Estate-level occurrences: 0; occurrences without a matching resource row: 0.

Recorded severity mix	Occurrences
Info	1

What was observed
The audit recorded network security groups without a NIC or subnet association.

Why it matters
An unassociated NSG is not enforcing rules on those resources. It may be intentionally staged or left behind; the record does not establish that another resource lacks protection.

What to verify
Confirm whether the NSG is referenced by deployment templates or planned changes. Identify an owner before attaching or removing it.

Policy considerations
Review lifecycle and deployment ownership; do not infer cost savings from this inventory alone.

Where it is concentrated

Subscription	Affected resources
Production	1

1 affected resources are in rg-network (Production), the largest resolved group concentration for this check.

Evidence examples

- nsg-unused is not associated with any subnet or NIC

Showing 1 of 1 occurrences. The technical reference groups all occurrences by resource; original titles and stored evidence remain in the snapshot database and data exports.

Source https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Governance and operational evidence

Tag presence supports resource classification, but any-tag coverage is not an ownership, cost-allocation or compliance verdict. Required-tag findings describe the audit performed at collection time; today's configuration is not reapplied to an old snapshot.

9 of 18 resources carry any tag (50%). The application uses 60% as a tag-presence threshold only; passing it does not demonstrate that required tags or useful values exist.

Development has the lowest any-tag coverage at 0%. Start by confirming the required keys and the teams responsible for the untagged resources, then review coverage at resource-group level.

Coverage by subscription

Subscription	Tag coverage
Development	0%
Production	60%

Coverage by tag key

Share of the 9 tagged resources carrying each key.

Tag key	Resources	Share
env	9	100%

9 resources have stored required-tag findings. The missing keys below are historical audit evidence; they do not establish the complete policy that was configured.

Resource group	Non-compliant	Missed tags
Production / rg-app	6	env
Development / rg-dev	3	env

Monitoring and recovery evidence

0 logging destinations receive recorded connections from 0 distinct resources. 0 monitoring connections and 0 recovery or backup vaults are recorded.

Logging connections, monitoring resources and recovery vaults show installed or configured infrastructure. This snapshot does not contain backup job outcomes, restore tests, alert delivery tests, application health or utilisation. Assign those checks separately before drawing an operational assurance conclusion.

Operational checks to complete

Confirm which services require central logging, verify that telemetry arrives and alerts reach an accountable team, and record the last successful restore test for each recovery-critical workload. Review retention and replication against the organisation's own recovery objectives.

Operational and compliance evidence

Microsoft service evidence recorded during collection. Results cover only the accessible scope; an empty dataset is not proof of zero cost, compliance, protection or service enablement. Detailed records remain in the snapshot database and data exports.

Azure Advisor cost opportunities

Currency	Period	Items	Savings	Annual savings
GBP	Month	1	125.50	Unknown

Collection: Recorded evidence

Estimates from Azure Advisor, grouped by currency and reported period. Annual estimates are separate. Missing amounts or periods remain unknown. Recommendations can overlap; totals are not guaranteed savings or billed costs.

Azure Policy evaluation states

Sub. ID	Assignment	Initiative ID	State	Results
sub-prod	/subscriptions/sub-prod/providers/microsoft.authorization/policyassignments/baseline	/providers/microsoft.authorization/policysetdefinitions/security-baseline	Exempt	1

Collection: Recorded evidence

Counts are policy evaluations, not distinct resources. Recorded states stay separate; missing evaluations never imply compliance. Full assignment and initiative IDs identify each group. A missing initiative may indicate a standalone policy or missing evidence.

Azure Policy exemptions

Category	Expiry at collection	Exemptions
Waiver	Due after 90 days	1

Collection: Recorded evidence

Expiry is assessed at collection time. Review expired exemptions and those due within 90 days with their owners. No expiry specified does not mean permanent approval; assignment scope and justification remain in the stored evidence.

Defender regulatory standards

Standard	State	Standard records
Azure-Security-Benchmark	Failed	1

Collection: Recorded evidence

Standard states across accessible subscriptions. Detailed control counts remain in the stored evidence. Missing or unsupported coverage does not establish compliance or certification.

Defender regulatory controls

Standard	State	Control records
Azure-Security-Benchmark	Unsupported	1

Collection: Recorded evidence

Control states across accessible subscriptions, grouped by standard. Skipped, unsupported and unknown states remain distinct from passes. Full control IDs remain in the stored evidence.

Defender regulatory assessments

Standard	State	Checks	Passed	Failed	Skipped
Azure-Security-Benchmark	Failed	1	12	2	Unknown

Collection: Recorded evidence

Passed, failed and skipped counts are resource occurrences across assessments; resources can be counted more than once. Missing counts remain unknown. These assessments do not establish certification or compliance of unassessed resources.

Policy assignment inventory

Enforcement	Assignments
Default	1
DoNotEnforce	1

Collection: Recorded evidence

Assignment inventory includes the requested inherited scope. Enforcement mode and excluded scopes affect interpretation; an assignment does not establish a passing evaluation.

Patch assessments

OS	State	Checks	Security updates	Critical updates
Linux	Succeeded	1	2	Unknown

Collection: Recorded evidence

Counts describe pending updates at the recorded assessment time and may overlap across classifications. Missing counts remain unknown. ARG assessment history is limited to seven days.

Backup and restore outcomes

Operation	State	Jobs
Backup	CompletedWithWarnings	1
Restore	Failed	1

Collection: Recorded evidence

Backup and restore jobs retain the provider status, including warnings. ARG exposes up to 14 days of jobs; an empty result does not prove successful backups.

Recent ARM changes

Type	Actor type	Events
Update	Application	1

Collection: Recorded evidence

Recorded ARM changes can include actor, client and changed properties. ARG retains 14 days; this is not a complete activity or data-plane audit log.

Policy evaluation coverage

Assignment	Name	State	Results
/subscriptions/sub-prod/providers/microsoft.authorization/policyassignments/baseline	Production baseline	Evaluation observed	1
/subscriptions/sub-prod/providers/microsoft.authorization/policyassignments/not-evaluated	Pending initiative	No evaluation observed	0

Collection: Recorded evidence

Assignments are matched to stored policy states using full normalised ARM IDs. No observed evaluation is kept separate from compliance and from unavailable state collection.

Machine assessment coverage

Type	State	Resources
microsoft.compute/virtualmachines	Evaluation observed	1

Collection: Recorded evidence

Counts use the collected VM and Arc inventory, deduplicated by full ARM ID. No observed assessment may indicate missing service configuration, access or expired evidence; it is not a passed patch check.

Evidence age at collection

Query	Review age (hours)	State	Items
patch_assessments	72	Missing or invalid timestamp	1

Collection: Recorded evidence

Ages are evaluated at the snapshot timestamp using the threshold recorded with each query. Future, invalid and missing dates stay separate. Review thresholds are configurable and are not Microsoft retention guarantees.

Prioritised review actions

Use this register to organise review work. The order preserves recorded severity, then the number of affected resources; it is not a business-impact score or an automatic remediation schedule. Establish owners and change dependencies before implementation.

Recommended review	Severity	Affected resources
Verify internet-sourced NSG rules	High	1
Verify storage anonymous-access requirements	High	1
Verify application HTTPS enforcement	Medium	1
Resolve historical required-tag omissions	Low	9
Confirm the purpose of unassociated NSGs	Info	1

Operational checks to complete

Collection coverage

The report describes the selected stored snapshot. Successful zero-row queries, query failures and missing run evidence are different states. A completed collection does not establish that every Azure service or control was assessed.

Snapshot status: complete. 11 queries have successful run records, including 0 with zero rows; 0 failed and 4 have no recorded outcome.

Snapshot	`dced93ea-6655-418a-ac15-a87608cee6ab`
Collected	2026-09-15T17:34:04.175996+00:00
Tenant	`fixture-tenant`

Collected query	Outcome	Rows
Defender compliance assessments	Completed	1
Defender compliance controls	Completed	1
Defender compliance standards	Completed	1
Advisor cost recommendations	Completed	1
Policy assignments	Completed	2
Policy exemptions	Completed	1
Policy states	Completed	1
All resources	Completed	18
Resource changes	Completed	1
Patch assessments	Completed	1
Backup jobs	Completed	2

The collector observes resource configuration through Azure Resource Graph. Effective user access, application traffic, billing, runtime health, backup success and recovery testing require additional evidence. Missing queries or resource properties must not be interpreted as a passed control.

This guidance explains the check's subject. The original recorded evidence remains authoritative, including when a locally overridden query uses the same check name.