

00:00:00





80 Questions covered in previous parts



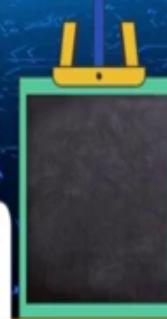
25 latest & important Questions



Get Certified  
**Build Cloud Career**



# The Tech BlackBoard



SUBSCRIBE



Share



@askthetechblackboard



@thetechblackboard



@Dtechblackboard

The Tech  
Blackboard

The Tech  
Blackboard

The Tech  
Blackboard



**Q81:** Which Azure Storage replication is the least expensive replication option?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

00:01:55 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X + https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy 160% Search Sign in

Microsoft Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events

Azure Product documentation ▾ Architecture ▾ Learn Azure ▾ Develop ▾ Resources ▾ Portal Free account

Filter by title recovery

- Data redundancy
- Customer-managed failover for disaster recovery
- > Access tiers and lifecycle management
- Object replication
- > Performance and scalability
- > Cost planning and optimization
- > Find, search, and understand blob data
- > Data migration
- > Monitoring
- > Disaster recovery

Download PDF

Learn / Azure / Storage /

# Azure Storage redundancy

Article • 12/28/2022 • 19 minutes to read • 30 contributors Feedback

## In this article

- Redundancy in the primary region
- Redundancy in a secondary region
- Read access to data in the secondary region
- Summary of redundancy options

Show 2 more

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

## Additional resources

### Training

Learning paths and modules

Provide disaster recovery by replicating storage data across regions and failing over to a...

Learn how to provide disaster recovery by replicating storage data across regions and failing over to a secondary location.

### Documentation

Hot, cool, and archive access tiers for blob data - Azure Storage

Azure storage offers different access tiers so that you can store your blob data in the most cost-effective manner based o...

Filter by title

RECOVERY

Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

exposed by that account. All storage resources deployed in the same storage account have the same redundancy setting. You may want to isolate different types of resources in separate storage accounts if they have different redundancy requirements.

## Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but isn't recommended for applications requiring high availability or durability.
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

### ⓘ Note

Microsoft recommends using ZRS in the primary region for Azure Data

**Q81:** Which Azure Storage replication is the least expensive replication option?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

**Q82:** Where does the copies of data maintained in LRS?

- a) Within a single region
- b) Across separate availability zones
- c) Secondary region
- d) Primary region and Secondary region

**Q81:** Which Azure Storage replication is the least expensive replication option?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

**Q82:** Where does the copies of data maintained in LRS?

- a) Within a single region
- b) Across separate availability zones
- c) Secondary region
- d) Primary region



Filter by title

RECOVERY

Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

exposed by that account. All storage resources deployed in the same storage account have the same redundancy setting. You may want to isolate different types of resources in separate storage accounts if they have different redundancy requirements.

## Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times **within a single physical location** in the primary region. LRS is the least expensive replication option, but isn't recommended for applications requiring high availability or durability.
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

### ⓘ Note

Microsoft recommends using ZRS in the primary region for Azure Data

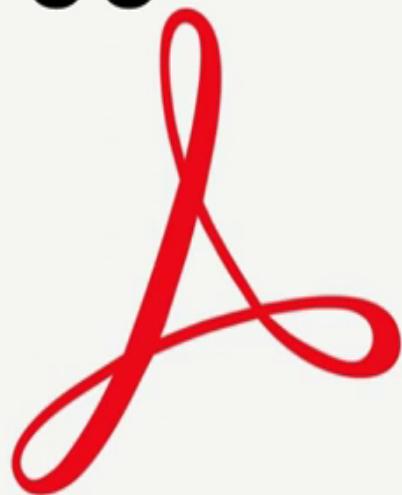
**Q81:** Which Azure Storage replication is the least expensive replication option?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

**Q82:** Where does the copies of data maintained in LRS?

- a) Within a single region
- b) Across separate availability zones
- c) Secondary region
- d) Primary region and Secondary region

Free



PDF

connectus@thetechblackboard.com

84

94

105.

Q93: Which Azure Storage replication comes under "Redundancy in the primary region"?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

**Q83:** Which Azure Storage replication comes under “Redundancy in the primary region”?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

redundancy requirements.

Filter by title

RECOVERY

Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

## Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but isn't recommended for applications requiring high availability or durability.
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

### Note

Microsoft recommends using ZRS in the primary region for Azure Data Lake Storage Gen2 workloads.

Download PDF

**Q83:** Which Azure Storage replication comes under “Redundancy in the primary region”?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)

**Q84:** Which Azure Storage replication comes under “Redundancy in a secondary region”?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS) 

- Customer-managed failover for disaster recovery
- > Access tiers and lifecycle management
- Object replication
- > Performance and scalability
- > Cost planning and optimization
- > Find, search, and understand blob data
- > Data migration
- > Monitoring
- > Protocol support
- Event handling
- Page blob features

[Download PDF](#)

## Redundancy in a secondary region

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If your storage account is copied to a secondary region, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

When you create a storage account, you select the primary region for the account. The paired secondary region is determined based on the primary region, and can't be changed. For more information about regions supported by Azure, see [Azure regions](#).

Azure Storage offers two options for copying your data to a secondary region:

- **Geo-redundant storage (GRS)** copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.
- **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the

## RECOVERY

## Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

## Redundancy in a secondary region

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If your storage account is copied to a secondary region, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

When you create a storage account, you select the primary region for the account. The paired secondary region is determined based on the primary region, and can't be changed. For more information about regions supported by Azure, see [Azure regions](#).

Azure Storage offers two options for copying your data to a secondary region:

- **Geo-redundant storage (GRS)** copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.
- **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the

Filter by title

RECOVERY

## Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

When you create a storage account, you select the primary region for the account. The paired secondary region is determined based on the primary region, and can't be changed. For more information about regions supported by Azure, see [Azure regions](#).

Azure Storage offers two options for copying your data to a secondary region:

- **Geo-redundant storage (GRS)** copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.
- **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.

### ⓘ Note

The primary difference between GRS and GZRS is how data is replicated in the primary region. Within the secondary region, data is always replicated synchronously three times using LRS. LRS in the secondary region protects your data against hardware failures.

times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.

- **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.

#### ① Note

The primary difference between GRS and GZRS is how data is replicated in the primary region. Within the secondary region, data is always replicated synchronously three times using LRS. LRS in the secondary region protects your data against hardware failures.

With GRS or GZRS, the data in the secondary region isn't available for read or write access unless there's a failover to the primary region. For read access to the secondary region, configure your storage account to use read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS). For more information, see [Read access to data in the secondary region](#).

If the primary region becomes unavailable, you can choose to fail over to the



**Q83:** Which Azure Storage replication comes under “Redundancy in the primary region”?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)



**Q84:** Which Azure Storage replication comes under “Redundancy in a secondary region”?

- a) Locally redundant storage (LRS)
- b) Zone-redundant storage (ZRS)
- c) Geo-redundant storage (GRS)
- d) Geo-zone-redundant storage (GZRS)



**Q85:** How many copies of data are maintained by an Azure Storage account that uses locally redundant storage?

3	4	6	9
---	---	---	---



**Three copies within a single region.**

**Q85:** How many copies of data are maintained by an Azure Storage account that uses locally redundant storage?

3	4	6	9
---	---	---	---



**Three copies within a single region.**

**Q86:** How many copies of data are maintained by an Azure Storage account that uses Zone-redundant storage (ZRS)?

3	4	6	9
---	---	---	---



**Three copies across separate availability zones within a single region**

The Tech  
Blackboard

The Tech  
Blackboard

o

The Tech  
Blackboard



**Q87:** How many copies of data are maintained by an Azure Storage account that uses Geo-redundant storage (GRS)/Read Access - Geo-redundant storage (RA-GRS)?

3	4	6	9
---	---	---	---



**Six copies total, including three in the primary region and three in the secondary region**

**Q87:** How many copies of data are maintained by an Azure Storage account that uses Geo-redundant storage (GRS)/Read Access - Geo-redundant storage (RA-GRS)?

3	4	6	9
---	---	---	---



**Six copies total, including three in the primary region and three in the secondary region**

**Q88:** How many copies of data are maintained by an Azure Storage account that uses Geo-zone-redundant storage (GZRS) / Read Access - Geo-zone-redundant storage (RA-GZRS)?

3	4	6	9
---	---	---	---



**Six copies total, including three across separate availability zones in the primary region and three locally redundant copies in the secondary region**

## Durability and availability parameters

The following table describes key parameters for each redundancy option:

**Filter by title****RECOVERY****Data redundancy**

Customer-managed failover

for disaster recovery

&gt; Access tiers and lifecycle management

Object replication

&gt; Performance and scalability

&gt; Cost planning and optimization

&gt; Find, search, and understand blob data

&gt; Data migration

&gt; Monitoring

&gt; Protocol support

Event handling

Page blob features

	for read requests	(99% for Cool or Archive access tiers)	(99% for Cool or Archive access tiers)	for Cool or Archive access tiers) for GRS	for Cool or Archive access tiers) f
				At least 99.99% (99.9% for Cool or Archive access tiers)	At least 99.99 (99.9% for Co Archive acces for RA-GZRS
Availability for write requests	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% for Cool or Ar access tiers)	At least 99.9% for Cool or Ar access tiers)

For more information, see the [SLA for Storage Accounts](#).

## Durability and availability by outage scenario

[Download PDF](#)



Parameter	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
Percent durability of objects over a given year	at least 99.999999999% (11 9's)	at least 99.999999999% (12 9's)	at least 99.99999999999999% (16 9's)	at least 99.999999999% (16 9's)
Availability for read requests	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers) for GRS	At least 99.9% (99.9% for Cool or Archive access tiers) for RA-GRS
Availability for write requests	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99.9% for Cool or Archive access tiers) for RA-GZRS
Number of copies of data maintained on separate	Three copies within a single region	Three copies across separate availability zones within a single region	Six copies total, including three in the primary region and three in the secondary region	Six copies total, including three in the separate availability zones in the region and three locally redundant copies in the secondary region



Filter by title

recovery

## Data redundancy

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

Redundancy tier	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
Standard	at least 99.9999999999% (11 9's)	at least 99.9999999999% (12 9's)	at least 99.99999999999999% (16 9's)	at least 99.99999999999999% (16 9's)
Archived	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers) for GRS At least 99.99% (99.9% for Cool or Archive access tiers) for RA-GRS	At least 99.9% (99% for Cool or Archive access tiers) for GZRS At least 99.99% (99.9% for Cool or Archive access tiers) for RA-GZRS
Locally redundant	Three copies within a single region	Three copies across separate availability zones	Six copies total, including three in the primary region and three in the secondary region	Six copies total, including three across separate availability zones in the primary region and three locally redundant

Filter by title

RECOVERY

**Data redundancy**

Customer-managed failover  
for disaster recovery

> Access tiers and lifecycle  
management

Object replication

> Performance and scalability

> Cost planning and optimization

> Find, search, and understand  
blob data

> Data migration

> Monitoring

> Protocol support

Event handling

Page blob features

Download PDF

	(99% for Cool or Archive access tiers)	(99% for Cool or Archive access tiers)	for Cool or Archive access tiers) for GRS	for Cool or Archive access tiers) for GZRS
ity	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers) for RA-GRS	At least 99.9% (99% for Cool or Archive access tiers) for RA-GZRS
f	Three copies within a single region	Three copies across separate availability zones	Six copies total, including three in the primary region and three in the secondary region	Six copies total, including three across separate availability zones in the primary region and three locally redundant copies in the secondary region
ied				

For more information, see the [SLA for Storage Accounts](#).

## Durability and availability by outage scenario

**Q89:** Which are Azure Storage access tiers?

- a) Hot tier
- b) Frequent tier
- c) Cool tier
- d) Cold tier
- e) Archive tier

**Q90:** Blob storage account and a general-purpose storage account, both are same.

True

False 



Azure

[Explore](#) [Products](#) [Solutions](#) [Pricing](#) [Partners](#) [Resources](#)[Learn](#) [Support](#) [Contact Sales](#)[Free account](#)[Sign in](#)[Home](#) / [Azure pricing](#) / [Azure Blob Storage pricing](#)

# Azure Blob Storage pricing

[Request a pricing quote](#)[Try Azure for free](#)[Storage Family](#) [Overview](#)[Pricing table](#)[Purchase options](#)[Resources](#)[FAQ](#)[Azure Blob Storage >](#)

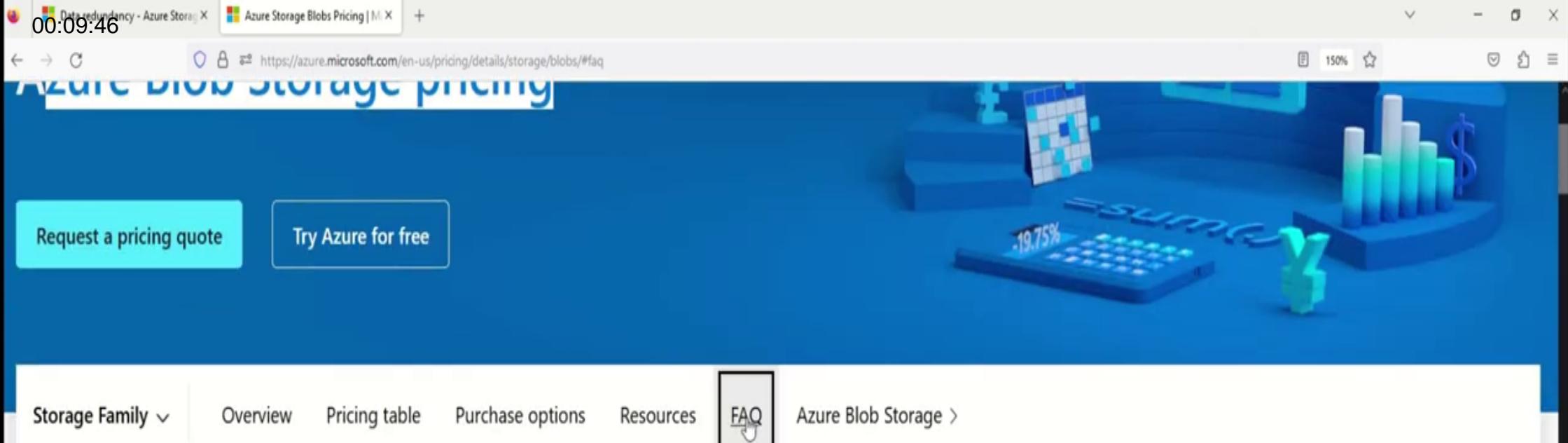
**Massively scalable and secure  
object storage**

Block blob storage is used for streaming and storing documents, videos, pictures, backups, and other unstructured text or binary data.

Total cost of block blob storage depends on:

• Volume of data stored per month

00:09:46 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X +

https://azure.microsoft.com/en-us/pricing/details/storage/blobs/#faq 150% The image shows the Azure Blob Storage Pricing page. At the top, there are two buttons: 'Request a pricing quote' and 'Try Azure for free'. The main content area features a blue background with a calculator, a bar chart, and a pound sign icon, all related to financial calculations. Below this, a navigation bar includes 'Storage Family ▾', 'Overview', 'Pricing table', 'Purchase options', 'Resources', and 'FAQ' (which is highlighted with a red box). A breadcrumb trail 'Azure Blob Storage >' follows.

## Massively scalable and secure object storage

Block blob storage is used for streaming and storing documents, videos, pictures, backups, and other unstructured text or binary data.

Total cost of block blob storage depends on:

- Volume of data stored per month.
- Quantity and types of operations performed, along with any data transfer costs.
- Data redundancy option selected.

00:09:49 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X +

File Structure Redundancy: Region: Currency:  
Hierarchical Namespace (NFS v3.0, SFTP Pr LRS West US 2 United States – Dollar (\$) USD

## Frequently asked questions

Frequently asked questions about Azure pricing >

### Blob storage

What is a Blob storage account, and how is it different from a general-purpose storage account? ▾

Have the prices for block blobs in general-purpose storage accounts changed? ▾

When looking at my Azure statement, how can I tell whether I'm being charged for a Blob Storage account, or blobs in General Purpose storage accounts? ▾

What are Premium Hot, Cool, and Archive access tiers, and how can I determine which one to use? ▾

Will I be charged for data reads if I toggle my Blob Storage or General Purpose v2 account from Cool to Hot? ▾

00:10:21 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X +

File Structure Redundancy: Region: Currency:

Hierarchical Namespace (NFS v3.0, SFTP Pr LRS West US 2 United States – Dollar (\$) USD

## Frequently asked questions

Frequently asked questions about Azure pricing >

### Blob storage

#### What is a Blob storage account, and how is it different from a general-purpose storage account?

A Blob Storage account is specialized for storing data as blobs, and allows users to specify an access tier based on the frequency of access to data in that account. General Purpose accounts can be used to store blobs as well as files, disks, tables, and queues.

#### Have the prices for block blobs in general-purpose storage accounts changed?

When looking at my Azure statement, how can I tell whether I'm being charged for a Blob Storage account, or blobs in General Purpose storage accounts?

What are Premium Hot, Cool, and Archive access tiers, and how can I determine which one to use?

**Q90:** Blob storage account and a general-purpose storage account, both are same.

True

False

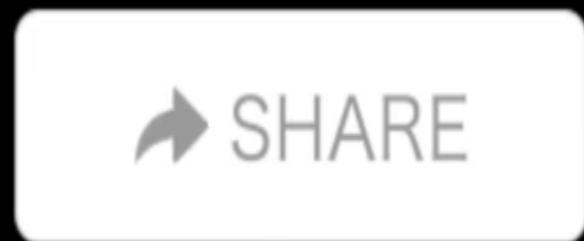
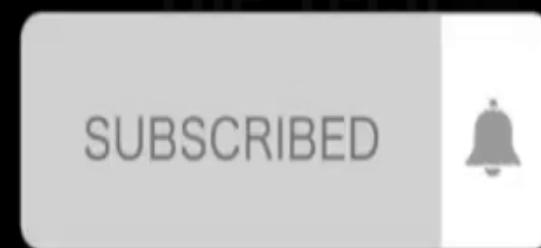
**Q90:** Blob storage account and a general-purpose storage account, both are same.

True

False



Like



Which page in Azure portal that you typically use to assign roles to grant access to Azure resources?

- a) Azure Active Directory (AAD)
- b) Policy hub
- c) User Access Management
- d) User Role Management

**Q91:** Which page in Azure portal that you typically use to assign roles to grant access to Azure resources?

- a) Access Control (IAM)
- b) Policy hub
- c) User Access Management
- d) User Role Management



Learn Documentation

Training

Certifications

Q&A

Code Samples

Assessments

Shows

Events

Search

Sign in

Azure

Product documentation

Architecture

Learn Azure

Develop

Resources

Portal

Free account

Filter by title

Azure RBAC documentation

> Overview

> Quickstarts

> Tutorials

> Concepts

✓ How-to guides

  List role definitions

  > List role assignments

  ✓ Assign roles

    Steps to assign a role

    ✓ Portal

      Assign roles

      Download documentation

      Download PDF

Learn / Azure / Role-based access control /



Additional resources

⊗ Training

Learning paths and modules

[Manage user roles - Training](#)

Manage user roles

Learning certificate

[Microsoft Certified: Identity and Access Administrator Associate - Certifications](#)

The Microsoft identity and access administrator designs, implements, and operates an organization's identity and...

## In this article

Prerequisites

[Step 1: Identify the needed scope](#)

[Step 2: Open the Add role assignment page](#)

[Step 3: Select the appropriate role](#)

[Show 4 more](#)

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

☰ Documentation

[Steps to assign an Azure role - Azure RBAC](#)





C

S

E

F

D

R

A

Z

P

L

I

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A

Z

Y

X

W

V

U

T

S

R

Q

P

O

N

M

H

G

F

E

D

C

B

A&lt;/div

00:11:45 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X Assign Azure roles using the Az... X Overview of dynamic members X +

Filter by title

Azure RBAC documentation

> Overview

> Quickstarts

> Tutorials

> Concepts

▽ How-to guides

- List role definitions
- > List role assignments
- ▽ Assign roles

Steps to assign a role

▽ Portal

- Assign roles
- Subscription administrator
- Managed identity
- External guest users

Download PDF

Security Policies Properties Locks Cost Management Cost analysis Cost alerts (preview) Budgets

Name Type Location

storage001122 Storage account East US

Page 1 of 1

## Step 2: Open the Add role assignment page

Access control (IAM) is the page that you typically use to assign roles to grant access to Azure resources. It's also known as identity and access management (IAM) and appears in several locations in the Azure portal.

1. Click Access control (IAM).

The following shows an example of the Access control (IAM) page for a resource group.

Home > Resource groups > example-group

example-group | Access control (IAM) ...

Resource group

Search (Ctrl+ /) Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags

Check access Role assignments Roles Deny assignments Classic administrators

My access

View my access

00:15:59 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X Assign Azure roles using the Az... X Overview of dynamic members X +

Filter by title

Azure RBAC documentation

> Overview

> Quickstarts

> Tutorials

> Concepts

▽ How-to guides

List role definitions

> List role assignments

▽ Assign roles

Steps to assign a role

▽ Portal

Assign roles

Subscription administrator

Managed identity

External guest users

Download PDF

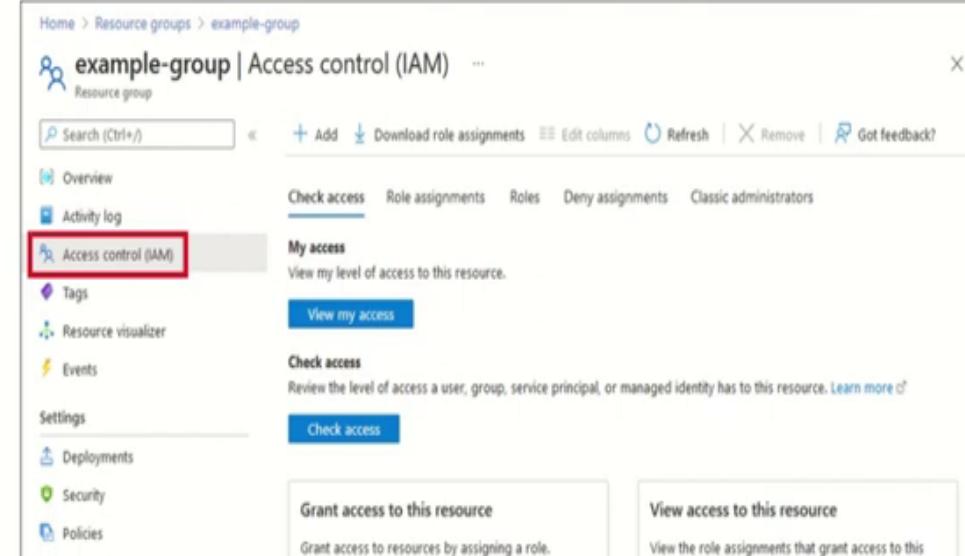
Budgets

## Step 2: Open the Add role assignment page

Access control (IAM) is the page that you typically use to assign roles to grant access to Azure resources. It's also known as identity and access management (IAM) and appears in several locations in the Azure portal.

1. Click Access control (IAM).

The following shows an example of the Access control (IAM) page for a resource group.



**Q91:** Which page in Azure portal that you typically use to assign roles to grant access to Azure resources?

- a) Access Control (IAM)
- b) Policy hub
- c) User Access Management
- d) User Role Management

**Q91:** Which page in Azure portal that you typically use to assign roles to grant access to Azure resources?

- a) Access Control (IAM)
- b) Policy hub
- c) User Access Management
- d) User Role Management

The screenshot shows the Azure portal interface for managing access to a resource group named "example-group". The left sidebar lists various management options like Overview, Activity log, and Access control (IAM). The "Access control (IAM)" option is highlighted with a red box. The main content area displays several sections: "Check access", "Role assignments", "Roles", "Deny assignments", and "Classic administrators". A prominent "My access" section allows users to view their level of access. Below it, a "Check access" button is available for users to review access levels for specific identities. Two main call-to-action boxes are present: "Grant access to this resource" (with "Add role assignment" and "Learn more" buttons) and "View access to this resource" (with "View" and "Learn more" buttons). Additionally, there are sections for "View deny assignments" and "Create a custom role".

**Q92:** Azure Active directory lets you set dynamic membership rules.

True

False



Learn

Documentation

Training

Certifications

Q&A

Code Samples

Assessments

Shows

Events

Search

Sign in

Filter by title

... items

Overview of dynamic membership for teams

Best practices for organizing teams in Teams

Manage large Teams

Create an org-wide team in Teams

Create people manager teams

Manage teams and channel policies

Turn off Teams Native File Upload policy

Manage Loop components

Manage actionable activity emails

Share to Teams from Outlook

Download PDF

Learn / Microsoft Teams /

+

In this article

Related topics

# Overview of dynamic membership for teams

Article • 12/01/2022 • 2 minutes to read • 14 contributors • Applies to: Microsoft Teams

Feedback

Microsoft Teams supports teams associated with Microsoft 365 groups by using *dynamic membership*. Dynamic membership enables the membership of a team to be defined by one or more rules that check for certain user attributes in Azure Active Directory (Azure AD). Users are automatically added or removed to the correct teams as user attributes change or users join and leave the tenant.

With dynamic membership you can set up teams for certain cohorts of users in your organization. Possible scenarios include:

- A hospital can create distinct teams for nurses, doctors, and surgeons to broadcast communications. This is especially important if the hospital

# Overview of dynamic membership for teams

Article • 12/01/2022 • 2 minutes to read • 14 contributors • Applies to: Microsoft Teams

 Feedback

Microsoft Teams supports teams associated with Microsoft 365 groups by using *dynamic membership*. Dynamic membership enables the membership of a team to be defined by one or more rules that check for certain user attributes in Azure Active Directory (Azure AD). Users are automatically added or removed to the correct teams as user attributes change or users join and leave the tenant.

With dynamic membership you can set up teams for certain cohorts of users in your organization. Possible scenarios include:

A hospital can create distinct teams for nurses, doctors, and surgeons to broadcast communications. This is especially important if the hospital relies on temp employees.

A university can create a team for all faculty within a particular college, including an adjunct faculty that changes frequently.

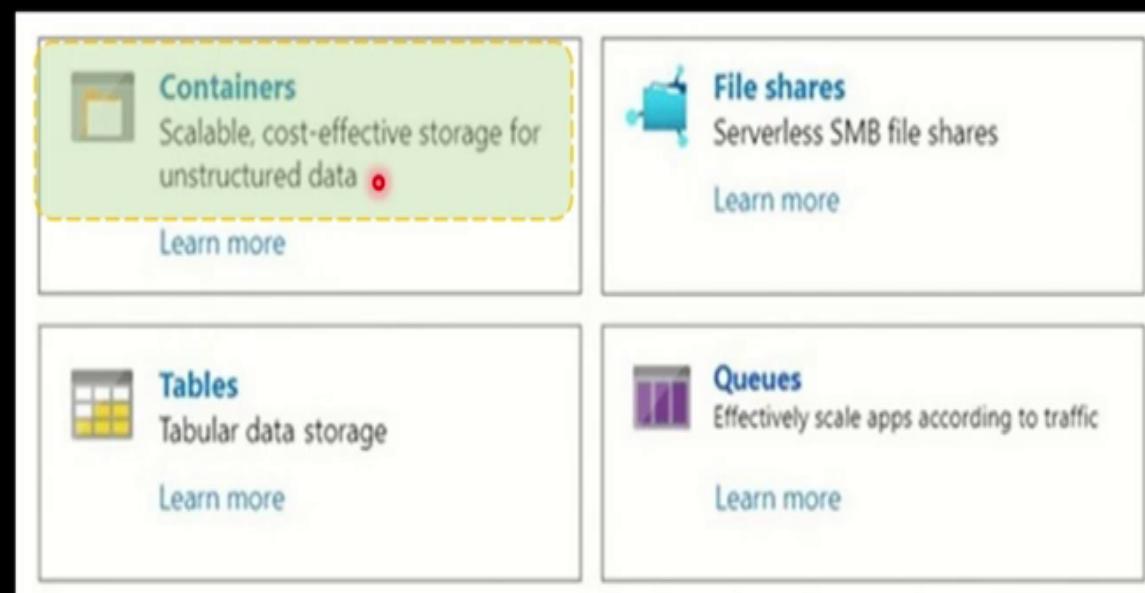
An airline wants to create a team for each flight (like a Tuesday afternoon)

**Q92:** Azure Active directory lets you set dynamic membership rules.

True

False

**Q93:** You plan to create an Azure virtual machine. You need to identify which storage service must be used to store the unmanaged data disks of the virtual machine. **What should you identify?**



The screenshot shows four service cards from the Azure portal:

- Containers**: Scalable, cost-effective storage for unstructured data. Includes a "Learn more" link.
- File shares**: Serverless SMB file shares. Includes a "Learn more" link.
- Tables**: Tabular data storage. Includes a "Learn more" link.
- Queues**: Effectively scale apps according to traffic. Includes a "Learn more" link.

**Q94:** Which cloud models can you deploy physical servers to?

- a) public cloud
- b) private cloud, hybrid cloud and public cloud
- c) hybrid cloud only
- d) private cloud and hybrid cloud

**Q95:** Azure pay-as-you-go pricing is an example of CapEx.

True

False

**Q96:** Paying electricity for your datacenter is an example of OpEX.

True

False

00:15:50 Data redundancy - Azure Storage X Azure Storage Blobs Pricing | M X Assign Azure roles using the A... X Overview of dynamic members X CapEx vs Opex - Microsoft Q&A X +

https://learn.microsoft.com/en-us/answers/questions/412063/capex-vs-opex 160% 160%

Microsoft Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events Search Sign in

Q&A Questions Tags FAQ & Help Ask a question

# CapEx vs Opex

asked May 27, 2021, 12:18 PM



Brenton Oberholzer

46

Please explain the difference between CapEx vs OpEx?

Is paying electricity every month for your datacenter a Capital or Operational Expense?

Not Monitored

1



I have the same question

3



Lucy Montague

6

Aug 3, 2022, 7:13 PM

Activity

Sign in to follow questions and users

# CapEx vs OpEx

asked May 27, 2021, 12:18 PM



Brenton Oberholzer

46

Please explain the difference between CapEx vs OpEx?

Is paying electricity every month for your datacenter a Capital or Operational Expense?

Not Monitored

1



I have the same question

3



Lucy Montague

6

Aug 3, 2022, 7:13 PM

The major difference between CAPEX and OPEX can be identified with the question: "Is what you are buying or intend to buy an asset? An Asset is something you can either sell or keep to gain continuous value from it. For example - An asset is the server in the data center, or even the software and the databases on the servers. Electricity is not an asset. The company cannot own it. It is seen as an OPEX.

This can become tricky when we are looking at XaaS. Software as a service

Not Monitored

1



I have the same question

3



Lucy Montague

6

Aug 3, 2022, 7:13 PM

The major difference between CAPEX and OPEX can be identified with the question: "Is what you are buying or intend to buy an asset? An Asset is something you can either sell or keep to gain continuous value from it. For example - An asset is the server in the data center, or even the software and the databases on the servers. Electricity is not an asset. The company cannot own it.

It is seen as **OPEX**.

This can become tricky when we are looking at XaaS. Software as a service (SaaS) for example is something the company never owns, and as such OPEX.

Having to maintain the code on top of the SaaS, could be CAPEX.

article on it - <https://viewpoint.pwc.com/dt/gx/en/pwc>

[INT/in\\_depths\\_INT/Configuration-and.html](#)

**Q97:** Deploying your own datacenter is an example of CapEx.

True

False.

**Q98:** Azure provides flexibility between capital expenditure (CapEx) and operational expenditure (OpEx).

True

False

**Q99:** When an Azure virtual machine is stopped, you continue to pay storage costs associated to the virtual machine.

True

False



6



**Q100:** An Azure resource can have multiple locks.

True

False

**Q101:** If an Azure resource has a Read-only lock, you can add a Delete lock to the resource?

Yes

No

**Q102:** An Azure resource inherits locks from its resource group.

True

False

# Lock inheritance

Filter by title

Manage Azure resources  
documentation

> Overview

> Concepts

▽ How to

> Move resources

> Tags

> Private link access

> Manage resource groups

> Manage resources

Resource providers and types

Preview features

Delete resource groups and  
resources

Lock resources

Authenticate across tenants

Download PDF

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the same parent lock. The most restrictive lock in the inheritance takes precedence.

Extension resources inherit locks from the resource they're applied to. For example, Microsoft.Insights/diagnosticSettings is an extension resource type. If you apply a diagnostic setting to a storage blob, and lock the storage account, you're unable to delete the diagnostic setting. This inheritance makes sense because the full resource ID of the diagnostic setting is:

JSON

Copy

```
/subscriptions/{sub-id}/resourceGroups/{rg-name}/providers/Microsoft.St
```

Which matches the scope of the resource ID of the resource that is locked:

JSON

Copy

```
/subscriptions/{sub-id}/resourceGroups/{rg-name}/providers/Microsoft.St
```

If you have a Delete lock on a resource and attempt to delete its resource group, the feature blocks the whole delete operation. Even if the resource

**Q102:** An Azure resource inherits locks from its resource group.

True

False

**Q103:** ReadOnly means authorized users can read a resource, but they can't delete or update it.

True

False

[Learn](#)[Documentation](#)[Training](#)[Certifications](#)[Q&A](#)[Code Samples](#)[Assessments](#)[Shows](#)[Events](#) Search[Sign in](#)[Azure](#) Product documentation ▾ Architecture ▾ Learn Azure ▾ Develop ▾ Resources ▾[Portal](#)[Free account](#)

Filter by title

- > Tags
- > Private link access
- > Manage resource groups
- > Manage resources

Resource providers and types

Preview features

Delete resource groups and resources

**Lock resources**

Authenticate across tenants

Throttling requests

Track asynchronous operations

Control plane metrics in Azure

Download PDF

[Learn](#) / [Azure](#) / [Resource Manager](#) / [Management](#) /**Additional resources**

# Lock your resources to protect your infrastructure

Article • 12/13/2022 • 12 minutes to read • 22 contributors

Feedback

## In this article

[Lock inheritance](#)[Understand scope of locks](#)[Considerations before applying your locks](#)[Who can create or delete locks](#)[Show 3 more](#)

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

Documentation

[Understand resource locking - Azure Blueprints](#)

Learn about the locking options in Azure Blueprints to protect resources when assigning a blueprint.

[Policy definitions for tagging resources - Azure Resource Manager](#)

Describes the Azure Policy definitions that you can assign to ensure tag compliance.

[Tag resources, resource groups, and subscriptions for logical organization - Azure Resource...](#)

Shows how to apply tags to organize

## Filter by title

- > [Tags](#)
- > [Private link access](#)
- > [Manage resource groups](#)
- > [Manage resources](#)
- [Resource providers and types](#)
- [Preview features](#)
- [Delete resource groups and resources](#)
- Lock resources**
- [Authenticate across tenants](#)
- [Throttling requests](#)
- [Track asynchronous operations](#)
- [Control plane metrics in Azure](#)
- > [Monitor](#)
- > [Reference](#)
- > [Resources](#)

[Download PDF](#)

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

You can set locks that prevent either deletions or modifications. In the portal, these locks are called **Delete** and **Read-only**. In the command line, these locks are called **CanNotDelete** and **ReadOnly**.

- **CanNotDelete** means authorized users can read and modify a resource, but they can't delete it.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the **Reader** role provides.

Unlike role-based access control (RBAC), you use management locks to apply a restriction across all users and roles. To learn about setting permissions for users and roles, see [Azure RBAC](#).

## Lock inheritance

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the same parent lock. The most restrictive lock in the inheritance takes precedence.

and subscriptions for logical organization - Azure Resource...

Shows how to apply tags to organize Azure resources for billing and managing.

Show 5 more

**Q103:** ReadOnly means authorized users can read a resource, but they can't delete or update it.

True

False

**Q104:** Which built-in roles can create and delete management locks.

- a) Owner
- b) Contributor
- c) User Access Administrator
- d) Reader

Filter by title

Manage Azure resourcesdocumentation> Overview> Concepts< How to> Move resources> Tags> Private link access> Manage resource groups> Manage resourcesResource providers and typesPreview featuresDelete resource groups and  
resourcesLock resourcesAuthenticate across tenantsDownload PDF

need to follow certain steps to clean up the stale links before you can protect the VM. For more information, see Troubleshoot Azure VM replication.

## Who can create or delete locks

To create or delete management locks, you need access to `Microsoft.Authorization/*` or `Microsoft.Authorization/locks/*` actions. Only the **Owner** and the **User Access Administrator** built-in roles can create and delete **management locks**. You can create a custom role with the required permissions.

## Managed applications and locks

Some Azure services, such as Azure Databricks, use managed applications to implement the service. In that case, the service creates two resource groups. One is an unlocked resource group that contains a service overview. The other is a locked resource group that contains the service infrastructure.

If you try to delete the infrastructure resource group, you get an error stating that the resource group is locked. If you try to delete the lock for the infrastructure resource group, you get an error stating that the lock can't be deleted because a system application owns it.

**Q104:** Which built-in roles can create and delete management locks.

- a) Owner
- b) Contributor
- c) User Access Administrator
- d) Reader

The Tech  
Blackboard



The Tech  
Blackboard



The Tech  
Blackboard

**Q105:** Delete and CanNotDelete, both locks achieve same objective. Users can read and modify a resource, but they can't delete it.

True

False

Filter by title

- > Tags
- > Private link access
- > Manage resource groups
- > Manage resources
- Resource providers and types
- Preview features
- Delete resource groups and resources
- Lock resources**
- Authenticate across tenants
- Throttling requests
- Track asynchronous operations
- Control plane metrics in Azure

Download PDF

Learn / Azure / Resource Manager / Management /

+

edit

⋮

Additional resources

# Lock your resources to protect your infrastructure

Article • 12/13/2022 • 12 minutes to read • 22 contributors

Feedback

## In this article

[Lock inheritance](#)

[Understand scope of locks](#)

[Considerations before applying your locks](#)

[Who can create or delete locks](#)

[Show 3 more](#)

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

Documentation

[Understand resource locking - Azure Blueprints](#)

Learn about the locking options in Azure Blueprints to protect resources when assigning a blueprint.

[Policy definitions for tagging resources - Azure Resource Manager](#)

Describes the Azure Policy definitions that you can assign to ensure tag compliance.

[Tag resources, resource groups, and subscriptions for logical organization - Azure Resource...](#)

Shows how to apply tags to organize

## In this article

 Filter by title

- > lags
  - > Private link access
  - > Manage resource groups
  - > Manage resources

## Resource providers and types

## Preview features

## Delete resource groups and resources

### **Lock resources**

Authenticate across tenants

### Throttling requests

### Track asynchronous operations

Control plane metrics in Azure

## Monitor

## > Reference

## > Resources

 Download PDF

### Lock inheritance

## Understand scope of locks

#### Considerations before applying your locks

Who can create or delete locks

Show 3 more

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

You can set locks that prevent either deletions or modifications. In the portal, these locks are called **Delete** and **Read-only**. In the command line, these locks are called `CannotDelete` and `ReadOnly`.

- **CanNotDelete** means authorized users can read and modify a resource, but they can't delete it.
  - **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the **Reader** role provides.

Unlike role-based access control (RBAC), you use management locks to apply a restriction across all users and roles. To learn about setting permissions for

Blueprints to protect resources when assigning a blueprint.

## Policy definitions for tagging resources - Azure Resource Manager

Describes the Azure Policy definitions that you can assign to ensure tag compliance.

Tag resources, resource groups, and subscriptions for logical organization - Azure Resource Manager

Shows how to apply tags to organize Azure resources for billing and managing.

Show 5 more

**Q105:** Delete and CanNotDelete, both locks achieve same objective. Users can read and modify a resource, but they can't delete it.

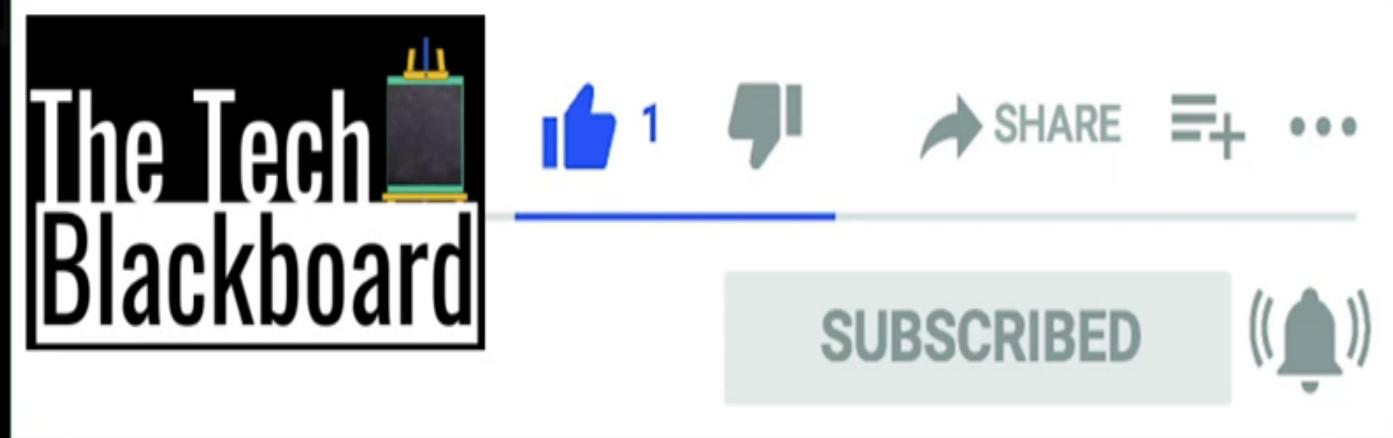
True

False

**Q105:** Delete and CanNotDelete, both locks achieve same objective. Users can read and modify a resource, but they can't delete it.

True

False



Connect with us



@askthetechblackboard



@thetechblackboard



@Dtechblackboard

**Q105:** Delete and CanNotDelete, both locks achieve same objective. Users can read and modify a resource, but they can't delete it.

True

False



Connect with us



@askthetechblackboard



@thetechblackboard



@Dtechblackboard



Blackboard