Azure Fundamentals & Administration

14 August 2022 10:00

About Rahul Joshi:

22 Years exp, 15th year as Microsoft certified trainer & AWS Authorized instructor

- Helping customers add Application Modernization capabilities by Replatforming ASP.NET sites to Azure App Services, Rearchitecting of monolithic applications to microservices or containers.
- Reengineering of legacy applications to cloud-native apps with improved user experience.
- Designing cloud strategy, solution design, cloud adoption frameworks, app modernization and cloud migration.
- Develop Proof of Concept by working closely with Microsoft and Amazon Web Services and design frameworks for cloud adoption and Enterprise Architecture, Cloud Infrastructure/ Migrations.
- Responsible for Migration to Microsoft Azure (Brownfield and Greenfield Projects). In-Premise To Cloud Migration and Storage Migration.
- Perform Application Readiness Assessment, an investigation at application level in preparation for cloud deployment, to look at issues that will either block or detract from the application's abilities to fully utilize the cloud, then act on this report to ensure cloud readiness.
- Designing applications for scalability
- Migrating to PaaS & Container Architecture, Migrating from Traditional .NET Application Web Apps

"Executed more than 580+ Trainings engagements on Microsoft Azure for more than 220+ clients"

Google Drive Link:
https://drive.google.com/drive/folders/181ebdbVLk5xpLu5ArR__BFWeM9b3N2x3?usp=sharing

Recording:
Please Note, Post Session Completes Zoom Recording Link will be shared on WhatsApp, Download it from Zoom Directly. It will not be uploaded on Google Drive

One Note Documentation:
https://1drv.ms/u/s!Aht-oGFG3XwWgagy2dnZHuXQmk0wkg

Case Study
The customer is highly impressed with the way Azure Masters have demonstrated the usability of compute related services like VM, VMSS and also WebApp. The customer now has come up with a unique requirement. Data in today's world is precious and Data reliability, Redundancy is always a primary concern. The customer says, they have two varieties of data, 1st which is only to be stored for long term as part of audit requirement and will be rarely used and 2nd type of data is typically used for the purpose of "Analytics", so the customer is very confused how to store these varieties of data. The customer does not know anything on the "Storage Front" and want Azure Masters to educate and demonstrate the above requirement.

In this requirement the customer is very particular about the following

1. Security of the Data is a primary concern
2. Redundancy and Availability of Data is another big concern
3. Cost associated with Storing the data is a maximum concern.

STAR

Situation: Case Study

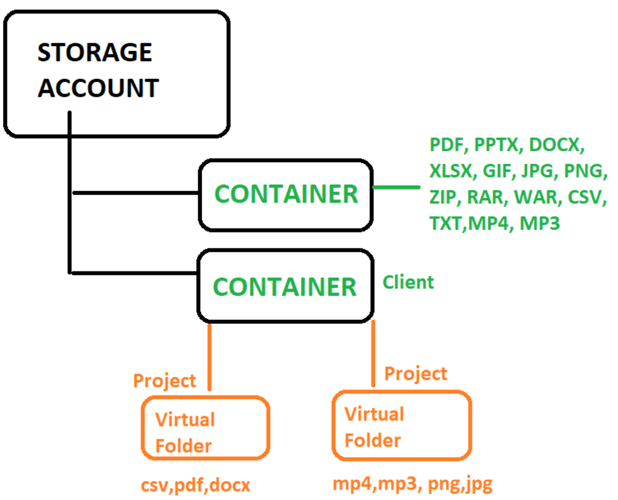
Task:

1. Create General Purpose V2 Storage Account
2. Create Data Lake Storage Gen 2 Storage Account

Azure — **STORAGE ACCOUNT** — AWS - **S3** - SIMPLE | SECURE | STORAGE

	GENERAL PURPOSE V2 STORAGE ACCOUNT	DEPRECATED ~~DATA LAKE STORAGE ACCOUNT GEN 1~~	DATA LAKE STORAGE ACCOUNT GEN 2
Purpose:	STORE | STORE | STORE THE DATA	~~Purpose: Store To Analyze Data~~ ~~Big Data | Hadoop~~	Purpose: Store To Analyze Data Big Data | Hadoop
Limit:	5 Petaytes - 5PB 1000 TB = 1 PB	~~Limit: NO LIMIT, INFINITE STORAGE~~ ~~Big Data - 3 V's Volume | Variety | Velocity~~	Limit: NO LIMIT, INFINITE STORAGE Big Data - 3 V's Volume | Variety | Velocity
Access Tier	HOT | COOL | ARCHIVE	~~Access Tier: HOT | COOL | ARCHIVE~~	HOT | COOL | ARCHIVE
Geo Replication Redundancy	LRS | GRS | ZRS | GZRS	~~Geo Replication Redundancy~~ ~~LRS | GRS | ZRS | GZRS~~	LRS | GRS | ZRS | GZRS

AZURE - STORAGE ACCOUNT



STORAGE ACCOUNT

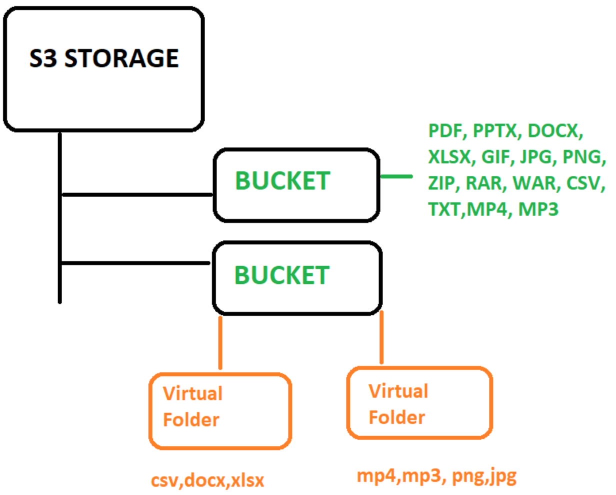
CONTAINER — PDF, PPTX, DOCX, XLSX, GIF, JPG, PNG, ZIP, RAR, WAR, CSV, TXT,MP4, MP3

CONTAINER — Client

Project — Virtual Folder — csv,pdf,docx

Project — Virtual Folder — mp4,mp3, png,jpg

AWS - S3 - SIMPLE SECURE STORAGE



S3 STORAGE

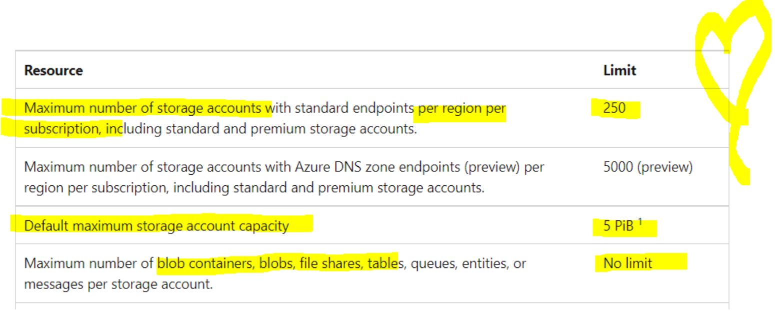
BUCKET — PDF, PPTX, DOCX, XLSX, GIF, JPG, PNG, ZIP, RAR, WAR, CSV, TXT,MP4, MP3

BUCKET

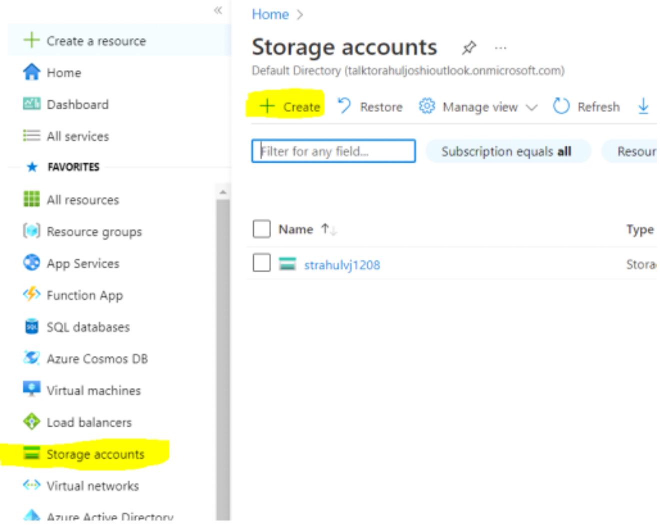
Virtual Folder — csv,docx,xlsx

Virtual Folder — mp4,mp3, png,jpg

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits



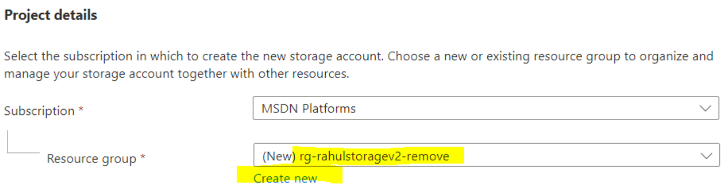
Resource	Limit
Maximum number of storage accounts with standard endpoints per region per subscription, including standard and premium storage accounts.	250
Maximum number of storage accounts with Azure DNS zone endpoints (preview) per region per subscription, including standard and premium storage accounts.	5000 (preview)
Default maximum storage account capacity	5 PiB [1]
Maximum number of blob containers, blobs, file shares, tables, queues, entities, or messages per storage account.	No limit



Storage accounts

Default Directory (talktorahuljoshioutlook.onmicrosoft.com)

Name	Type
strahulvj1208	Stora

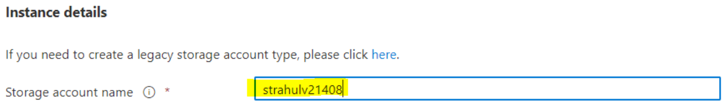


Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * MSDN Platforms

Resource group * (New) rg-rahulstoragev2-remove

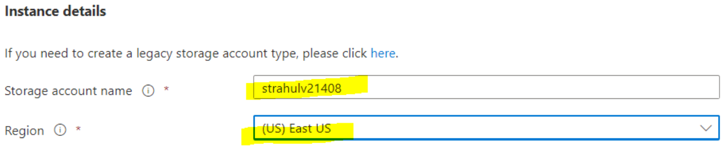


Instance details

If you need to create a legacy storage account type, please click here.

Storage account name ⓘ * strahulv21408

This Storage account name has to be unique because Microsoft behind the scene creates a **DNS Record** and you can get an address for this **storage account which you can access from the Internet**, because this address has to be unique, that is why the storage account name also has to be unique.



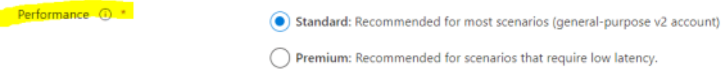
Instance details

If you need to create a legacy storage account type, please click here.

Storage account name ⓘ * strahulv21408

Region ⓘ * (US) East US

100% EXAM question - AZ-900, AZ-104

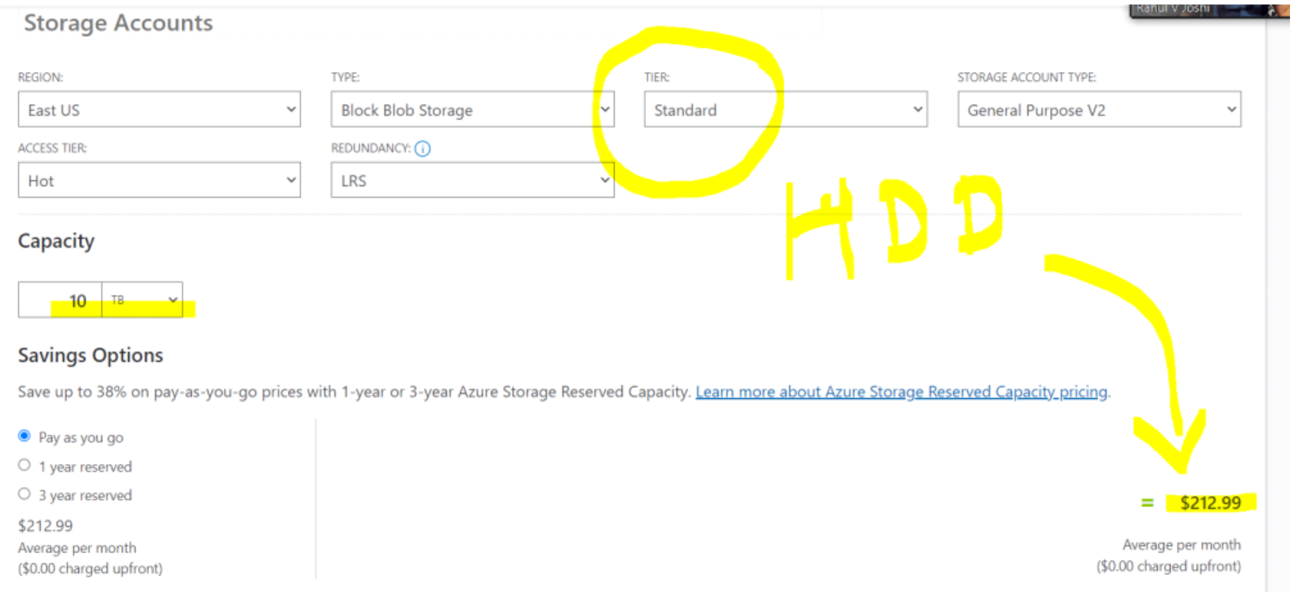


Performance ⓘ *

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

1. Standard - **VERY CHEAP STORAGE**, THIS IS BEST FOR **STORING THE DATA ONLY**, IT **USES MAGNETIC DISK**, **WHICH IS VERY CHEAP**. 99% OF THE TIMES, WE WILL ALWAYS USE "STANDARD"



Storage Accounts

REGION: East US

TYPE: Block Blob Storage

TIER: Standard

STORAGE ACCOUNT TYPE: General Purpose V2

ACCESS TIER: Hot

REDUNDANCY: LRS

Capacity

10 TB

Savings Options

Save up to 38% on pay-as-you-go prices with 1-year or 3-year Azure Storage Reserved Capacity. Learn more about Azure Storage Reserved Capacity pricing.

- ● Pay as you go
- ○ 1 year reserved
- ○ 3 year reserved

$212.99
Average per month
($0.00 charged upfront)

= $212.99

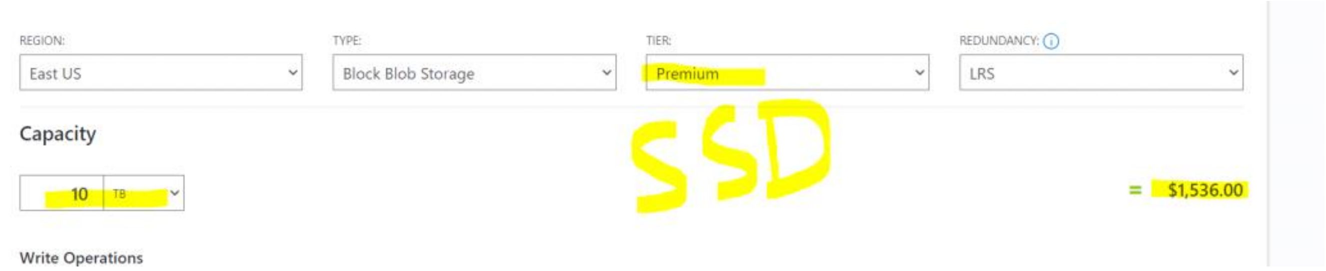
Average per month
($0.00 charged upfront)

2. Premium - EXPENSIVE STORAGE, WHEN YOU WANT FASTER READ / WRITE (IOPS - INPUT / OUTPUT PER SEC) - THIS USES SSD STORAGE, THEN ONLY YOU SHOULD PREMIUM

   - **Example**: If you want to Storage SQL Server Database on Storage Account and always Insert / Update / Delete / Select is going to happen then you use Premium

   - **Example:** If you want to store Virtual Machine's Hard Disk (VHD) on the Storage Account, then use Premium, because VM Hard Disk may require faster IOPS

   - **Example:** You want to store LOG Files, Remember Log Files are always Written to the End, if you application's LOG File has to be stored in Storage Account, Data has to be written in the log file vert fast, then use Premium



REGION: East US

TYPE: Block Blob Storage

TIER: Premium

REDUNDANCY: LRS

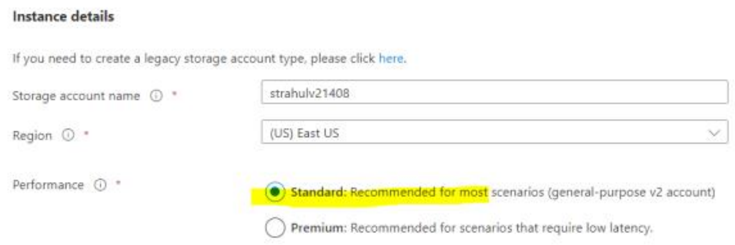
Capacity

10 TB

= $1,536.00

Write Operations

Block Blob - Page Blob - Append Blob - Comes Later



Instance details

If you need to create a legacy storage account type, please click here.

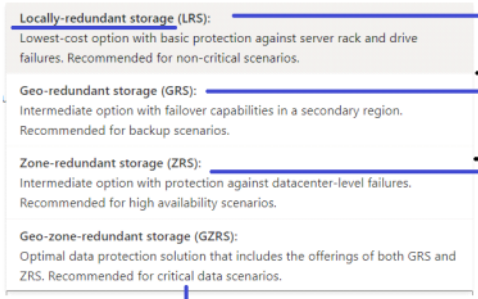
Storage account name ⓘ * strahulv21408

Region ⓘ * (US) East US

Performance ⓘ *
● Standard: Recommended for most scenarios (general-purpose v2 account)
○ Premium: Recommended for scenarios that require low latency.

EXAM Question + Interview Question:

Redundancy - SAFE GUARIND DATA, PROTECTING DATA



Locally-redundant storage (LRS):
Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios.

Geo-redundant storage (GRS):
Intermediate option with failover capabilities in a secondary region. Recommended for backup scenarios.

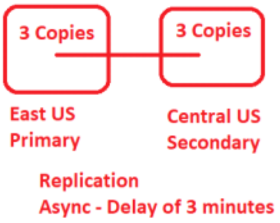
Zone-redundant storage (ZRS):
Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.

Geo-zone-redundant storage (GZRS):
Optimal data protection solution that includes the offerings of both GRS and ZRS. Recommended for critical data scenarios.

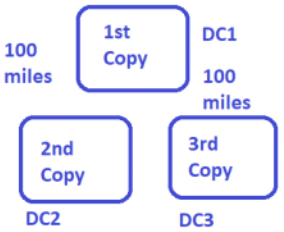
Lowest Redundancy - Cheapest

3 Copies of the Data are stored in the Same Datacenter, in different RACs. This is the Cheapest of All and if the Datacenter goes down, the data wont be available.

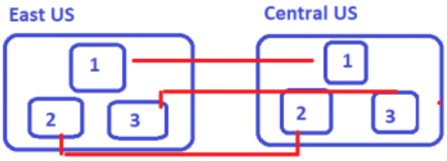
3 Copies are kept in the Primary Region and 3 Additional Copies are Kept in a Partner Region. You cannot choose the Partner, Microsoft selects Automatically. This is Expensive than LRS, as total 6 Copies are Kept



This option comes only when the Primary Region has 3 Datacenters.
1st DC - 1st Copy, 2nd DC - 2nd Copy, 3rd DC - 3rd Copy



Combination of GEO + ZRS (Highest Redundancy) (Most Expensive)



Cost Compare

10TB	LRS	$212.99	(3 Copies - 3 RACs)
10TB	ZRS	$266.24	(3 Copies in 3 Datacenters - Same Region)
10TB	GRS	$468.99	(6 Copies - 3 In 1 Region, 3 In Another Region)
10TB	G-ZRS	$479.23	(6 Copies - 3 In 1 Region 3 DC, 3 In Another Region - 3 DC)

Access Tier - HOT | COOL | ARCHIVE

10TB	LRS	HOT	$212.99
10TB	LRS	COOL	$155.65
10TB	LRS	ARCHIVE	$10.14

Data Compare

10TB	LRS	$212.99	(3 Copies - 3 RACs)
10TB	ZRS	$266.24	(3 Copies in 3 Datacenters - Same Region)
10TB	GRS	$468.99	(6 Copies - 3 In 1 Region, 3 In Another Region)
10TB	G-ZRS	$479.23	(6 Copies - 3 In 1 Region 3 DC, 3 In Another Region - 3 DC)

10TB	LRS	HOT	$212.99
10TB	LRS	COOL	$155.65
10TB	LRS	ARCHIVE	$10.14

Decide the Cost

Standard vs Premium

Redundancy

Access Tier

Partner Region Website:
https://docs.microsoft.com/en-us/azure/availability-zones/cross-region-replication-azure

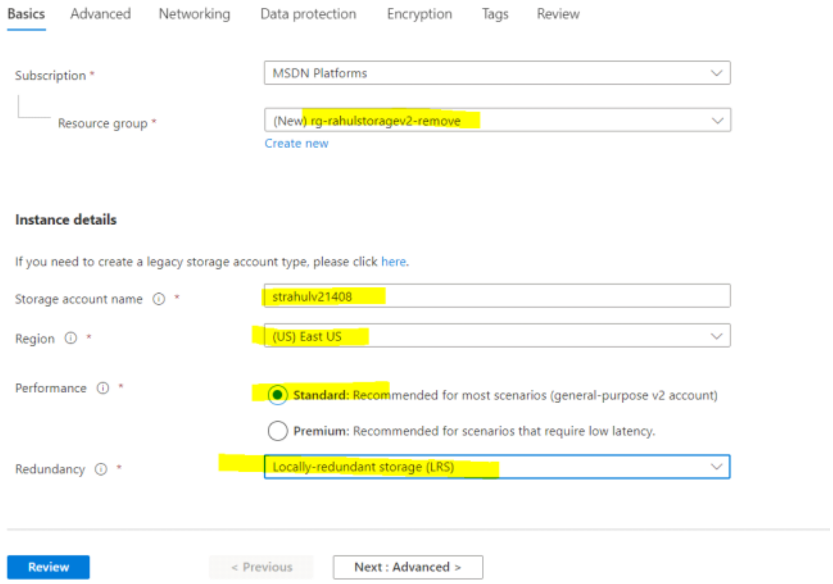
More Reading on Redundancy - EXAM Point | Architect
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

Access tier: Hot Cool Archive - - EXAM Point | Architect
https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview

- **Hot tier** - An online tier optimized for storing data that is accessed or modified frequently. The Hot tier has the highest storage costs, but the lowest access costs.

- **Cool tier** - An online tier optimized for storing data that is infrequently accessed or modified. Data in the Cool tier should be stored for a minimum of 30 days. The Cool tier has lower storage costs and higher access costs compared to the Hot tier.

- **Archive tier** - An offline tier optimized for storing data that is rarely accessed, and that has flexible latency requirements, on the order of hours. Data in the Archive tier should be stored for a minimum of 180 days.
Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge. :)



Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

Subscription * MSDN Platforms

Resource group * (New) rg-rahulstoragev2-remove

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name * strahulv21408

Region * (US) East US

Performance *

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy * Locally-redundant storage (LRS)

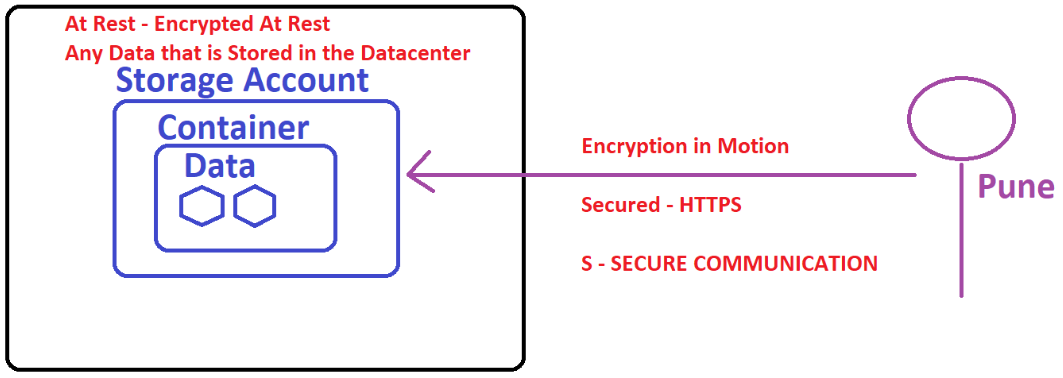
Create a storage account ...

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

Security

1. Access Control
2. Permissions
3. Auditing
4. Protecting Data
5. Encrypting Data

Azure Data Center - East US



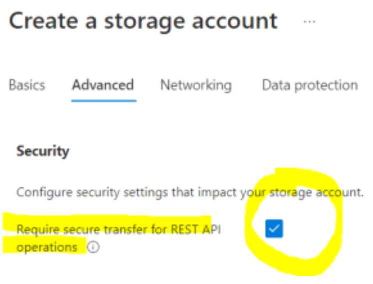
At Rest - Encrypted At Rest

Any Data that is Stored in the Datacenter

Encryption in Motion

Secured - HTTPS

S - SECURE COMMUNICATION



Create a storage account ...

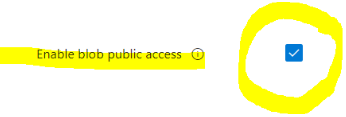
Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

Security

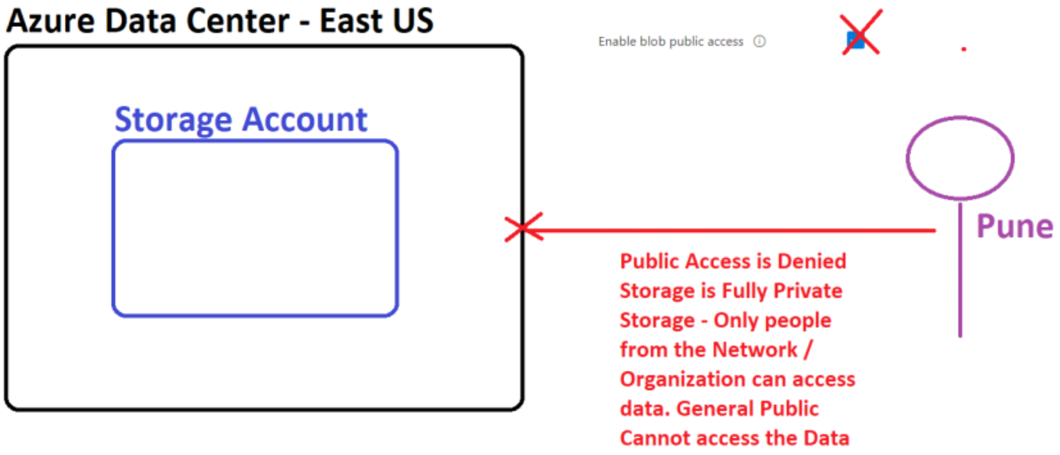
Configure security settings that impact your storage account.

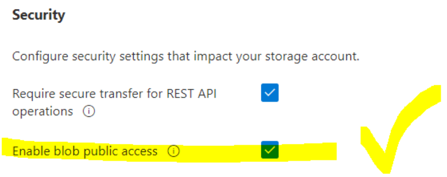
Require secure transfer for REST API operations ☑

The secure transfer option enhances the security of your storage account by only allowing REST API operations on the storage account using HTTPs. Any requests using HTTP will be rejected when this setting is enabled



Enable blob public access ⓘ ☑





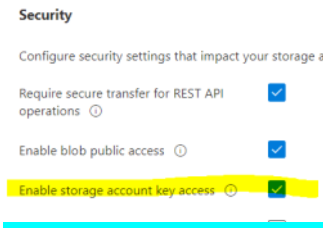
Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ ☑

Enable blob public access ⓘ ☑

Even if we tick this option, can we make the Individual Container "Private", if you make a Container "Private" anyways, people from the internet cannot access the container, but what if other containers are Public, this can be a security risk, so, if you want all the containers in the storage account to be Private by default, keep the option "Un Tick" do not select the option.



Security

Configure security settings that impact your storage account.

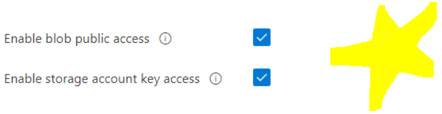
Require secure transfer for REST API operations ⓘ ☑

Enable blob public access ⓘ ☑

Enable storage account key access ⓘ ☑

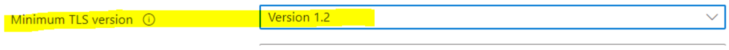
Using Storage Account Key, people can connect to the Storage Account, But if anyone Gets the Storage Account Key, they get Full Control over the Storage Account, They can Create, Delete, Add, Modify and do anything on the Storage Account, This option is very risky, so if you feel at organization level, no one should use Storage Account Key, then uncheck this option.

Security is a serious profession

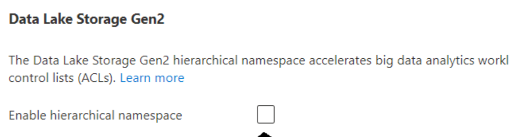


Enable blob public access ⓘ ☑

Enable storage account key access ⓘ ☑



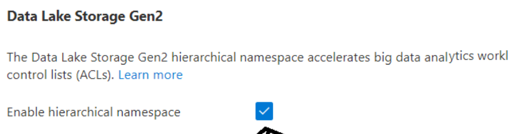
Minimum TLS version ⓘ Version 1.2



Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workl
control lists (ACLs). Learn more

Enable hierarchical namespace □



Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workl
control lists (ACLs). Learn more

Enable hierarchical namespace ☑

Store | Store | Store

5 PB Maximum

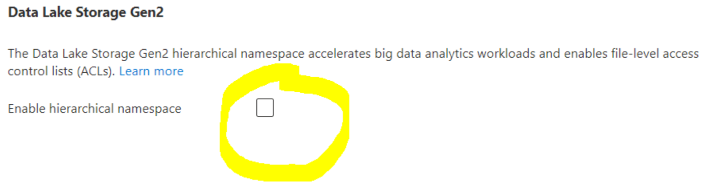
99% Used

Store + Analytics

Infinite Storage

Big Data | Hadoop

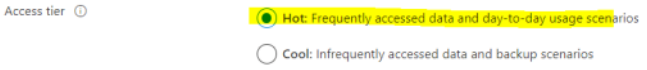
Training



Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). Learn more

Enable hierarchical namespace □

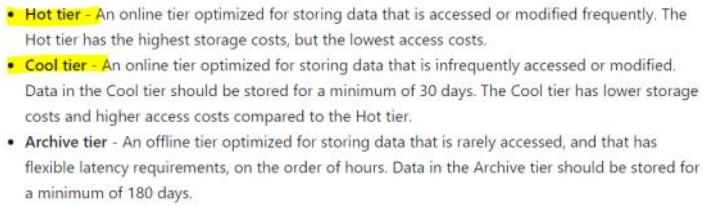


Access tier ⓘ

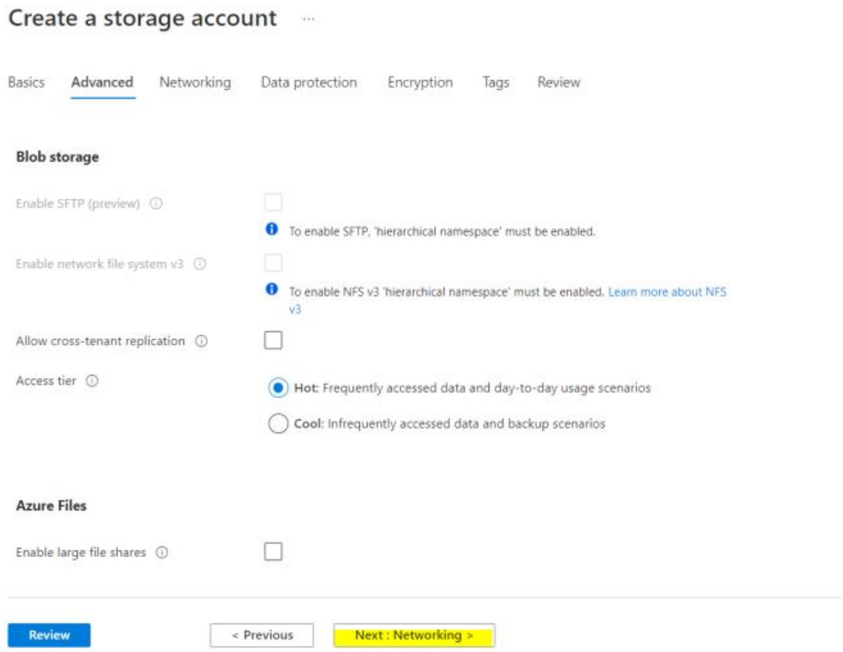
● **Hot:** Frequently accessed data and day-to-day usage scenarios

○ **Cool:** Infrequently accessed data and backup scenarios

Archive is not shown by default.



- **Hot tier** - An online tier optimized for storing data that is accessed or modified frequently. The Hot tier has the highest storage costs, but the lowest access costs.
- **Cool tier** - An online tier optimized for storing data that is infrequently accessed or modified. Data in the Cool tier should be stored for a minimum of 30 days. The Cool tier has lower storage costs and higher access costs compared to the Hot tier.
- **Archive tier** - An offline tier optimized for storing data that is rarely accessed, and that has flexible latency requirements, on the order of hours. Data in the Archive tier should be stored for a minimum of 180 days.



Create a storage account ...

Blob storage

Enable SFTP (preview) ⓘ □

ⓘ To enable SFTP, 'hierarchical namespace' must be enabled.

Enable network file system v3 ⓘ □

ⓘ To enable NFS v3 'hierarchical namespace' must be enabled. Learn more about NFS v3

Allow cross-tenant replication ⓘ □

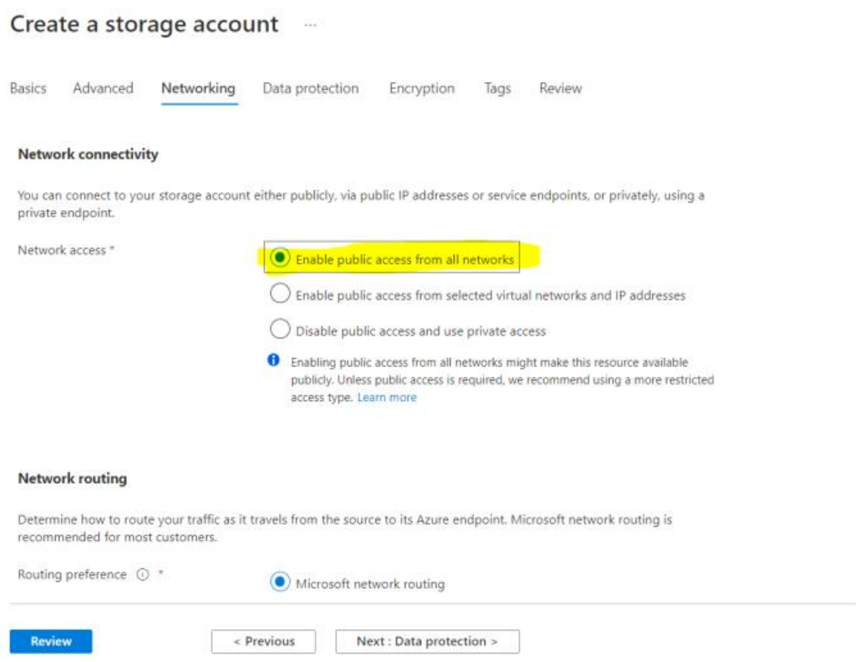
Access tier ⓘ

● **Hot:** Frequently accessed data and day-to-day usage scenarios

○ **Cool:** Infrequently accessed data and backup scenarios

Azure Files

Enable large file shares ⓘ □



Create a storage account ...

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

● Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

○ Disable public access and use private access

Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more

Network routing

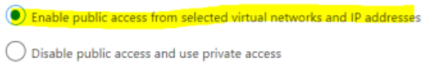
Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference ⓘ *

● Microsoft network routing

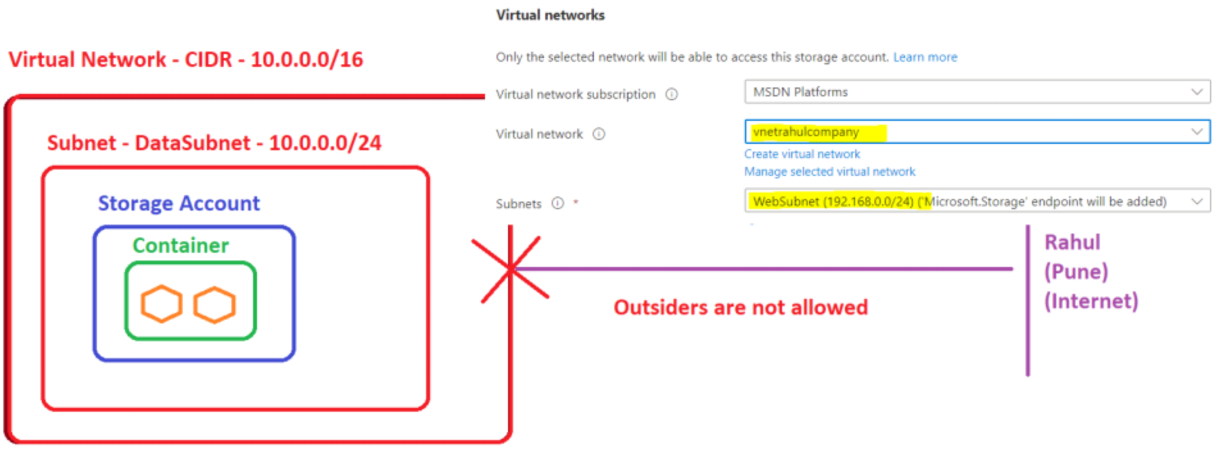
Any one from the internet, any network, can access the storage account, this can be very un-secure, but if you storage does not contain sensitive data, data is not important and even if it is accessed by public, it is fine, then this default option is good for you.,

But, if the storage contains, sensitive data which is used only by your organization and this data cannot be exposed to the general public, then you should fence the storage behind a network, like shown in the diagram below



● Enable public access from selected virtual networks and IP addresses

○ Disable public access and use private access



Virtual networks

Only the selected network will be able to access this storage account. Learn more

Virtual network subscription ⓘ: MSDN Platforms

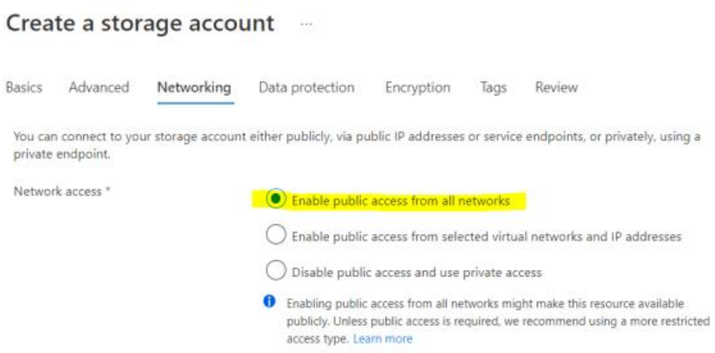
Virtual network ⓘ: vnetrahulcompany

Subnets ⓘ *: WebSubnet (192.168.0.0/24) ('Microsoft.Storage' endpoint will be added)

Create virtual network
Manage selected virtual network
Virtual Network - CIDR - 10.0.0.0/16
Subnet - DataSubnet - 10.0.0.0/24
Storage Account
Container
Outsiders are not allowed
Rahul
(Pune)
(Internet)

Firewall - Allowed IP Addresses - Rahul V Joshi's Public IP

Training:



Create a storage account ···

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

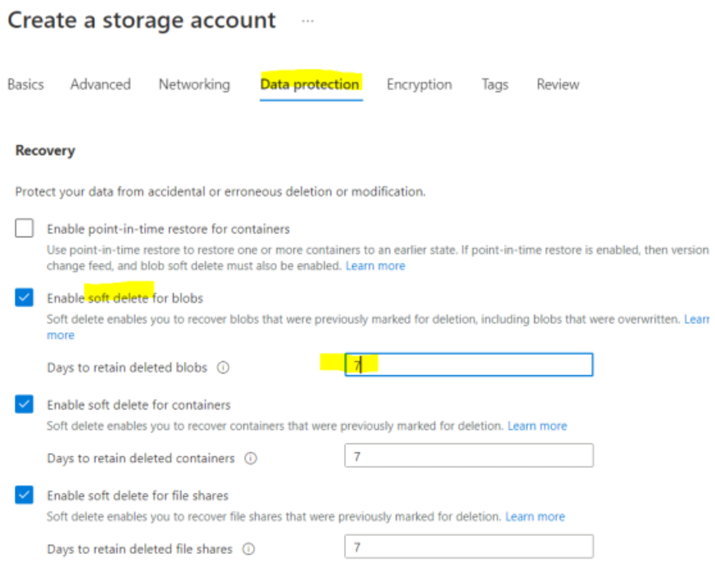
Network access *

● Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

○ Disable public access and use private access

Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more



Create a storage account ···

Recovery

Protect your data from accidental or erroneous deletion or modification.

□ Enable point-in-time restore for containers

Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then version change feed, and blob soft delete must also be enabled. Learn more

☑ Enable soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

Days to retain deleted blobs: 7

☑ Enable soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. Learn more

Days to retain deleted containers: 7

☑ Enable soft delete for file shares

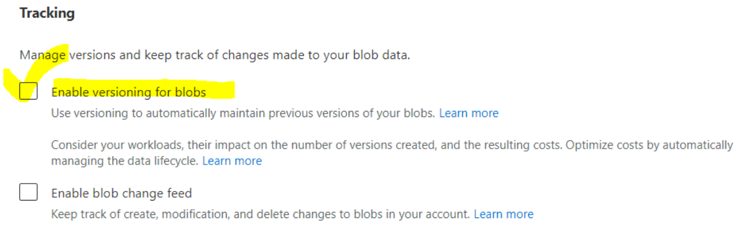
Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Days to retain deleted file shares: 7

You can Recovery data, within 7 Days, But, Data cannot be recovered after 7 Days. **Cost**, Even if the data is in Soft Delete, Microsoft Still Charges for the Data

Versioning

If you upload a file, by the same, the file gets overwritten, if you want to maintain multiple version of the file, you can enable versioning. Please Note, for every version - cost is applied, So, if you have 1TB File and you have 10 copies of it, you will be charged for 10TB (1 * 10 Versions)



Tracking

Manage versions and keep track of changes made to your blob data.

□ Enable versioning for blobs

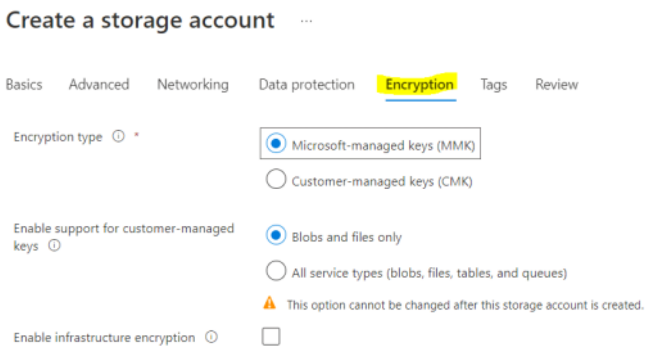
Use versioning to automatically maintain previous versions of your blobs. Learn more

Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. Learn more

□ Enable blob change feed

Keep track of create, modification, and delete changes to blobs in your account. Learn more

Encryption (Exam + Interviews)



Create a storage account ···

Encryption type *

● Microsoft-managed keys (MMK)

○ Customer-managed keys (CMK)

Enable support for customer-managed keys

● Blobs and files only

○ All service types (blobs, files, tables, and queues)

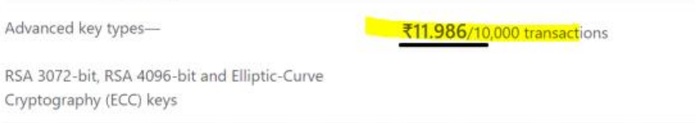
This option cannot be changed after this storage account is created.

Enable infrastructure encryption □

2048

3072

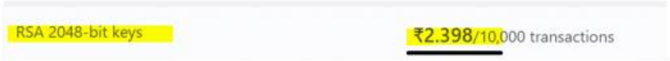
4096



Advanced key types—

₹11.986/10,000 transactions

RSA 3072-bit, RSA 4096-bit and Elliptic-Curve Cryptography (ECC) keys



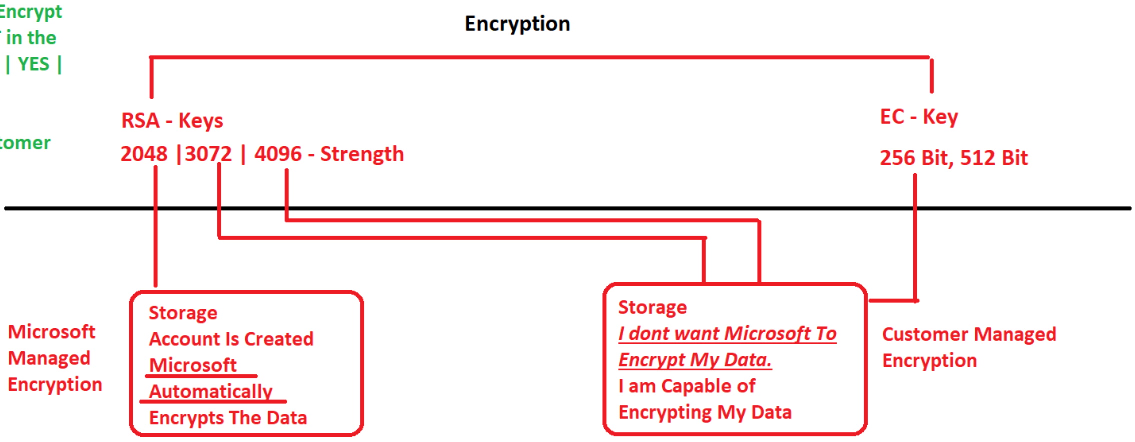
RSA 2048-bit keys

₹2.398/10,000 transactions

Does Microsoft Encrypt The Data at REST in the Datacenter? YES | YES | YES.

Can you as a customer take control

YES | YES | YES



Encryption

RSA - Keys

2048 |3072 | 4096 - Strength

EC - Key

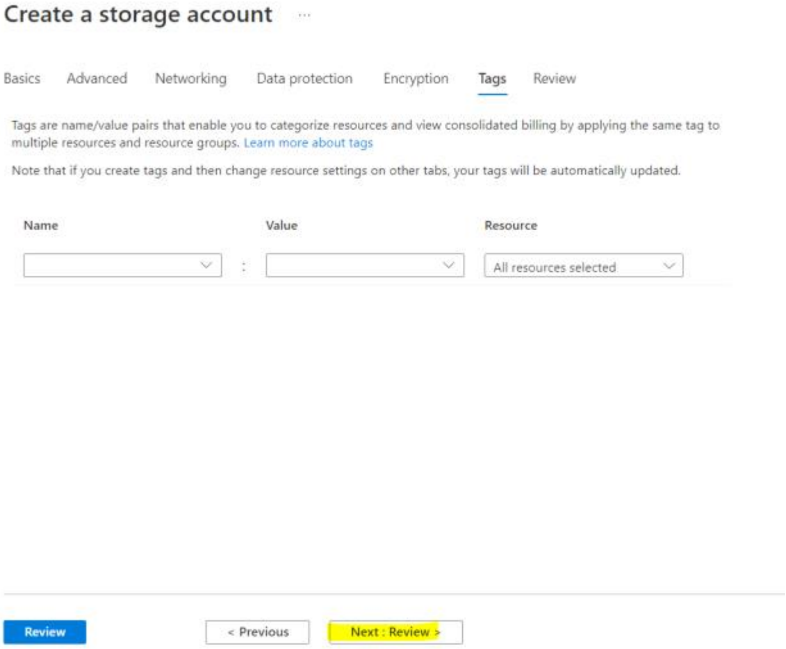
256 Bit, 512 Bit

Microsoft Managed Encryption

Storage Account Is Created Microsoft Automatically Encrypts The Data

Storage *I dont want Microsoft To Encrypt My Data.* I am Capable of Encrypting My Data

Customer Managed Encryption

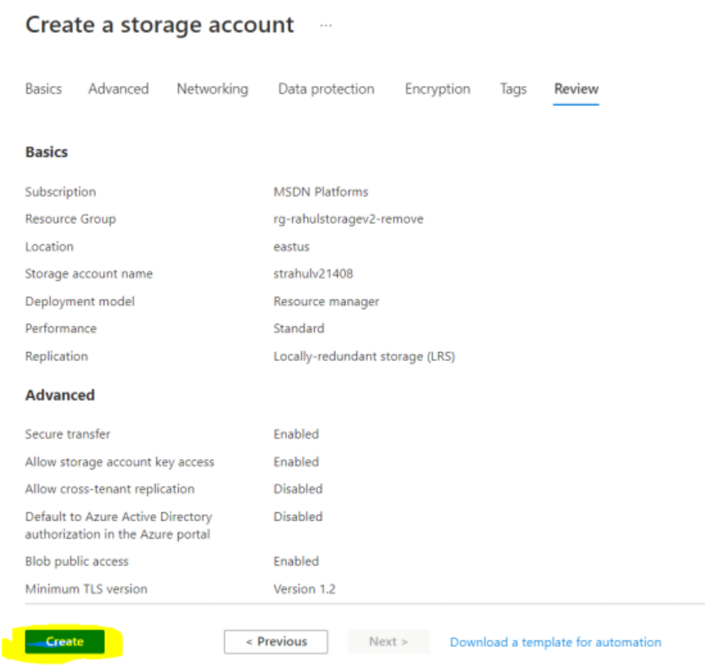


Create a storage account ···

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
		All resources selected



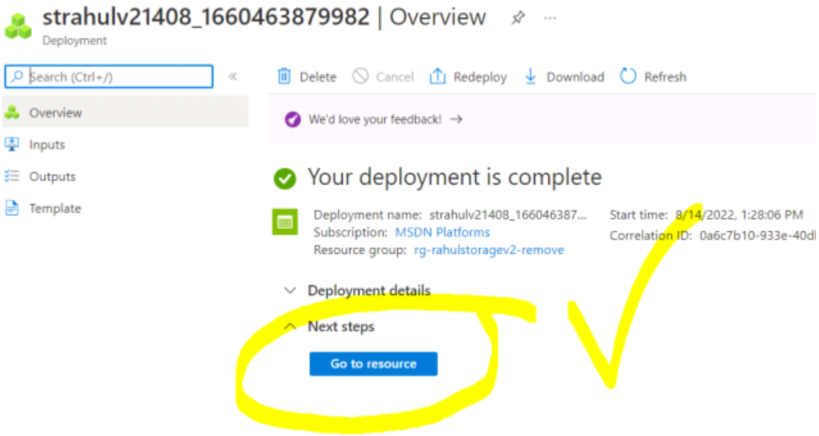
Create a storage account ···

Basics

Subscription	MSDN Platforms
Resource Group	rg-rahulstoragev2-remove
Location	eastus
Storage account name	strahulv21408
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Secure transfer	Enabled
Allow storage account key access	Enabled
Allow cross-tenant replication	Disabled
Default to Azure Active Directory authorization in the Azure portal	Disabled
Blob public access	Enabled
Minimum TLS version	Version 1.2



strahulv21408_1660463879982 | Overview

Deployment

Your deployment is complete

Deployment name: strahulv21408_166046387...
Subscription: MSDN Platforms
Resource group: rg-rahulstoragev2-remove

Start time: 8/14/2022, 1:28:06 PM
Correlation ID: 0a6c7b10-933e-40d

Case Study

The customer is very happy as we have created the Storage Account, but now has some important milestones to cross.

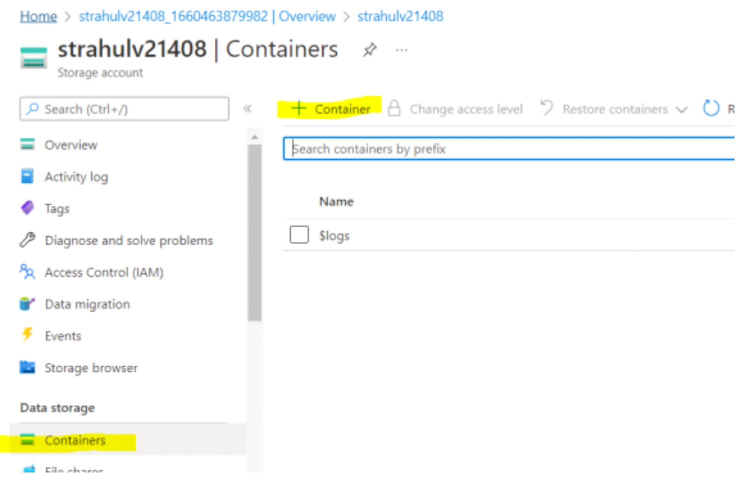
1. The customer has some data which is not sensitive and some data which is sensitive, both these types of data elements have to store in the same storage account.
2. The customer mentions that, by default they choose LRS as Redundancy, so they need to configure GRS as that was change as a decision.
3. The customer also mentions that After 30 days the file is last modified, the access tier should change to Cool and after 60 days from the last modified the Access tier should change to Archive and after 365 days, the file should be deleted. This should be done automatically.

Situation = Case Study

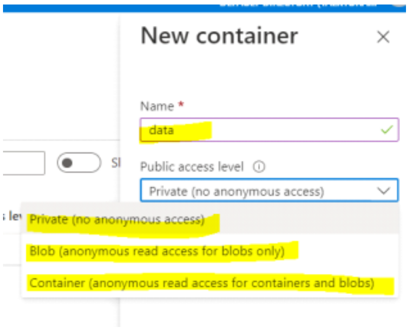
Task:

1. The customer has some data which is not sensitive and some data which is sensitive, both these types of data elements have to store in the same storage account.

Action:



Name
□ $logs



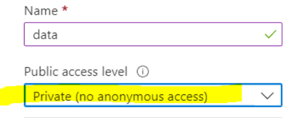
Name * data

Public access level ⓘ Private (no anonymous access)

Private (no anonymous access)
Blob (anonymous read access for blobs only)
Container (anonymous read access for containers and blobs)

Public Access Level
https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure?tabs=portal

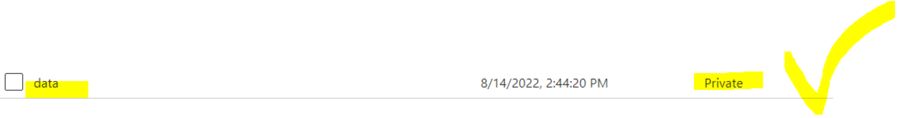
If you data in the container is highly sensitive data and should not be accessed by General Public from the Internet, you sho uld keep Private



Name * data

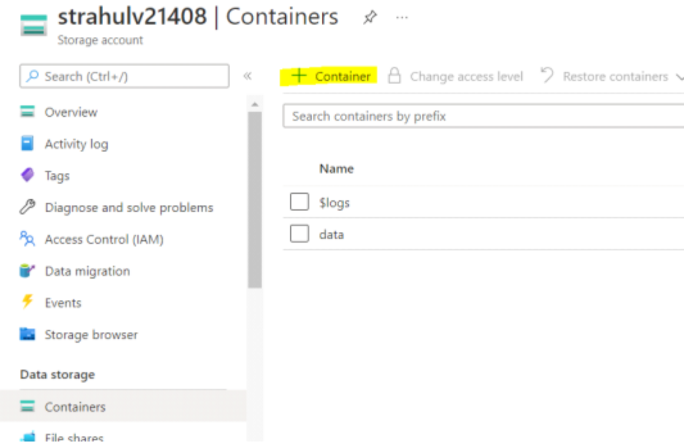
Public access level ⓘ Private (no anonymous access)

Click Create

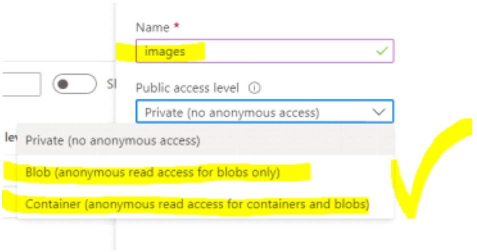


□ data 8/14/2022, 2:44:20 PM Private

Non-Sensitive Data - People from the Internet, who are not Authorized people, can also read the data from the data
Example: Amazon India website, Jio Mart



Name
□ $logs
□ data



Name *

images

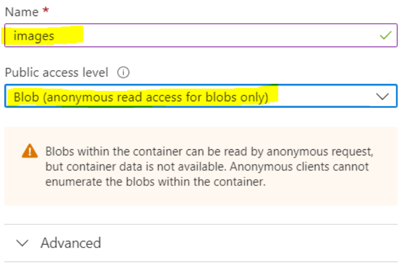
Public access level

Private (no anonymous access)

- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous read access for containers and blobs)

Public read access for blobs only: **Blobs within the container can be read** by anonymous request, but container data is not available anonymously. Anonymous clients cannot enumerate the blobs within the container.

Public read access for container and its blobs: **Container and blob data can be read** by anonymous request, except for container permission settings and container metadata. Clients can enumerate blobs within the container by anonymous request, but cannot enumerate containers within the storage account



Name *

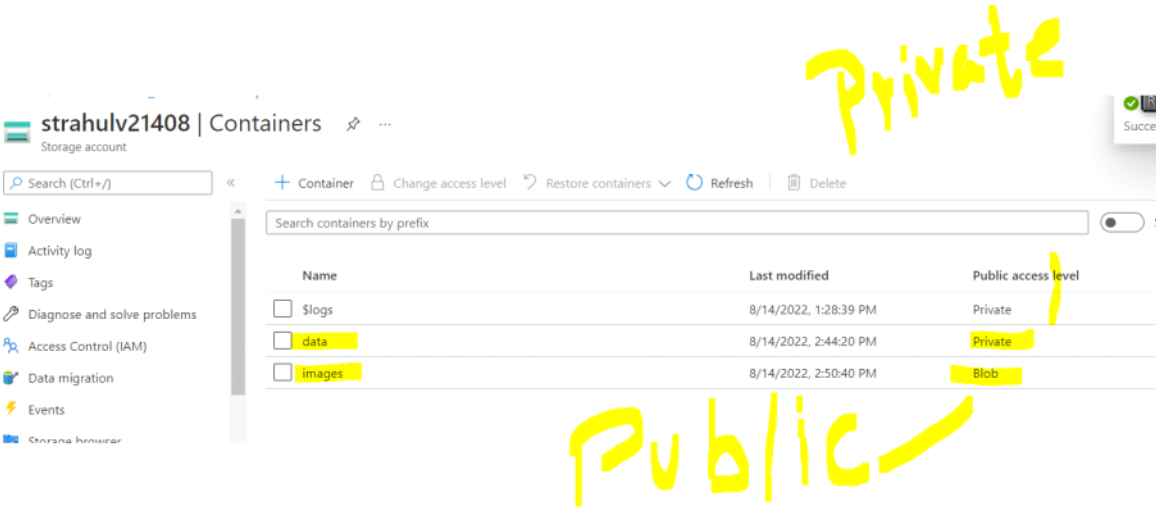
images

Public access level

Blob (anonymous read access for blobs only)

Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.

Advanced

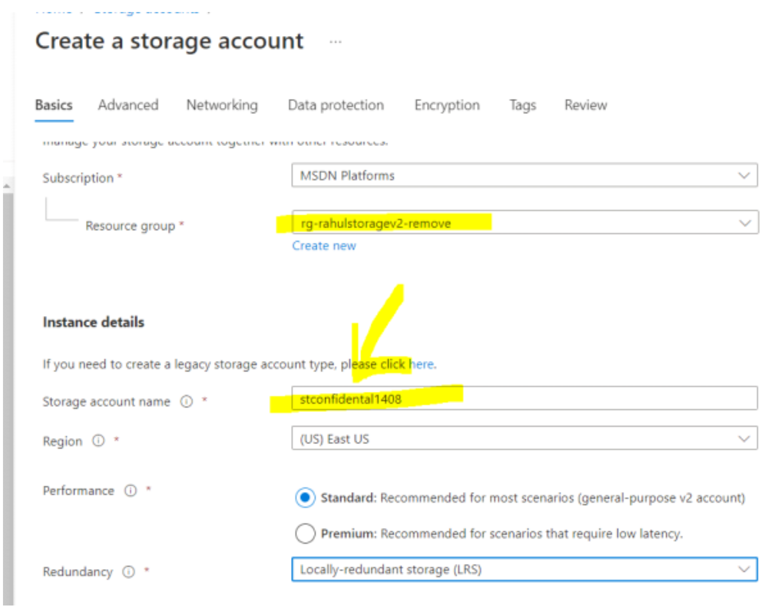


strahulv21408 | Containers

Storage account

Name	Last modified	Public access level
$logs	8/14/2022, 1:28:39 PM	Private
data	8/14/2022, 2:44:20 PM	Private
images	8/14/2022, 2:50:40 PM	Blob

Please Watch



Create a storage account

Subscription * MSDN Platforms

Resource group * rg-rahulstoragev2-remove

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name * stconfidental1408

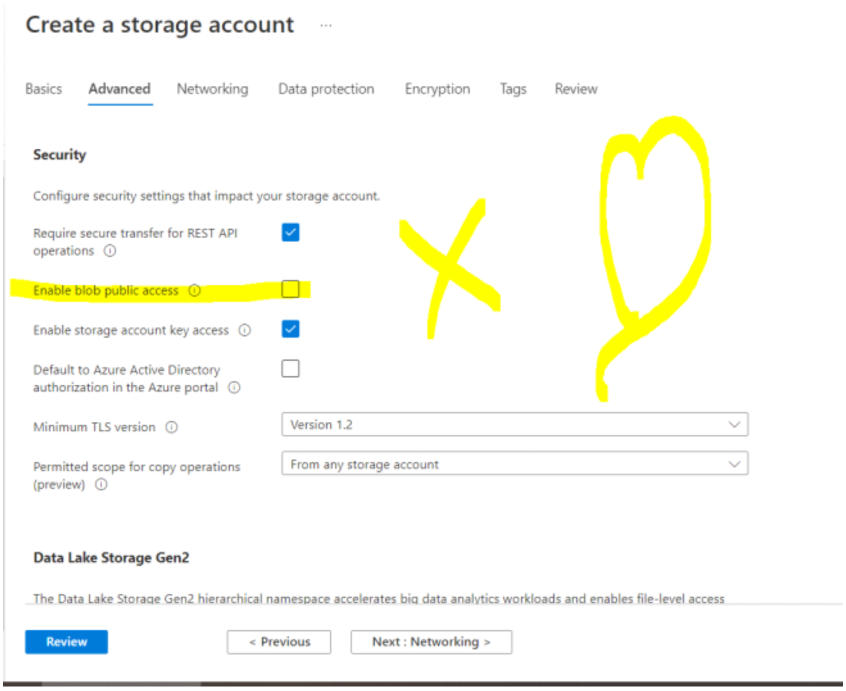
Region * (US) East US

Performance *

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy * Locally-redundant storage (LRS)



Create a storage account ···

Basics | **Advanced** | Networking | Data protection | Encryption | Tags | Review

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ ☑

Enable blob public access ⓘ ☐

Enable storage account key access ⓘ ☑

Default to Azure Active Directory authorization in the Azure portal ⓘ ☐

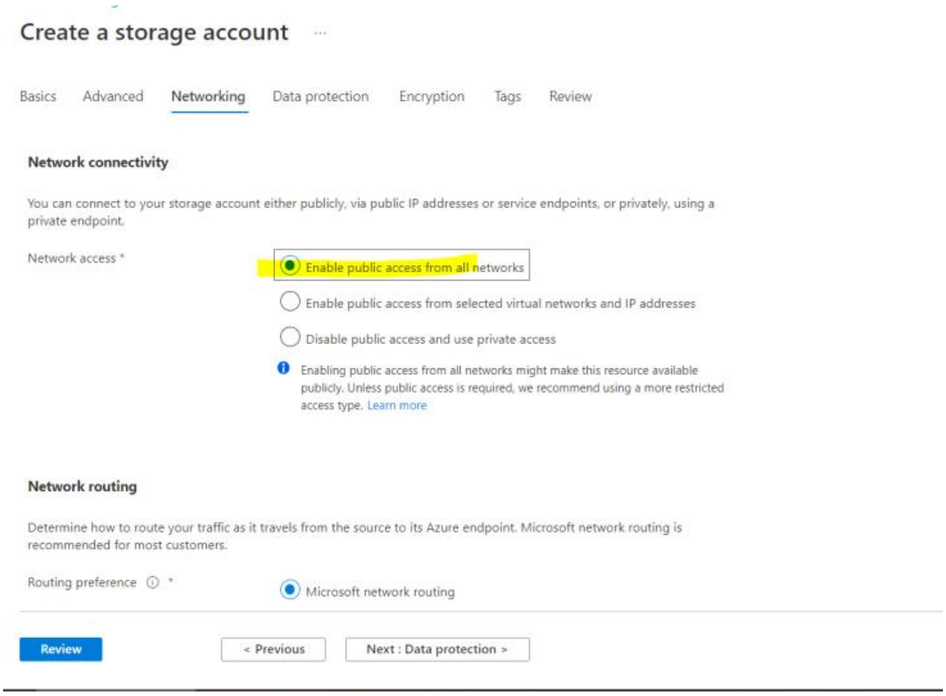
Minimum TLS version ⓘ: Version 1.2

Permitted scope for copy operations (preview) ⓘ: From any storage account

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access

No one from Public, Internet can access my data, very strict. Yes



Create a storage account ···

Basics | Advanced | **Networking** | Data protection | Encryption | Tags | Review

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

● Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

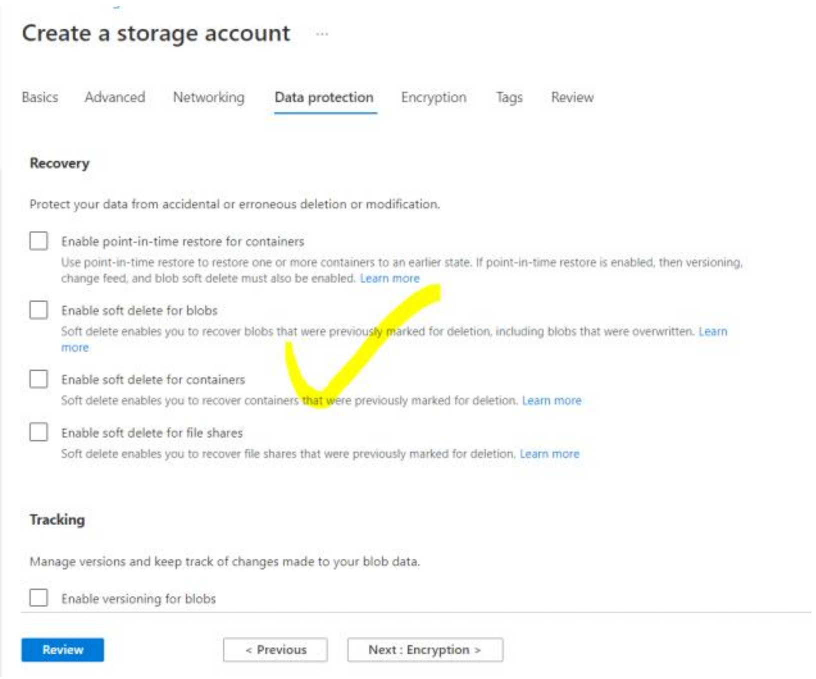
○ Disable public access and use private access

ⓘ Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference ⓘ * ● Microsoft network routing



Create a storage account ···

Basics | Advanced | Networking | **Data protection** | Encryption | Tags | Review

Recovery

Protect your data from accidental or erroneous deletion or modification.

□ Enable point-in-time restore for containers
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. Learn more

□ Enable soft delete for blobs
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

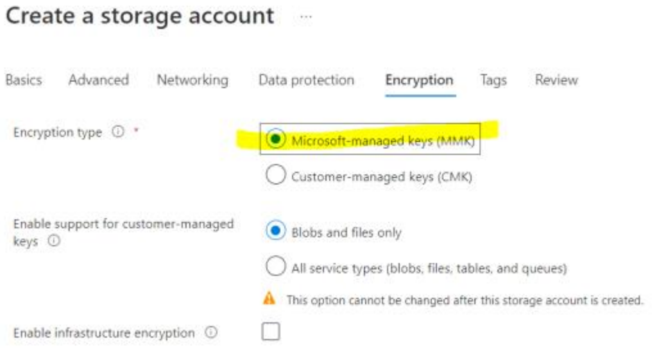
□ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. Learn more

□ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Tracking

Manage versions and keep track of changes made to your blob data.

□ Enable versioning for blobs



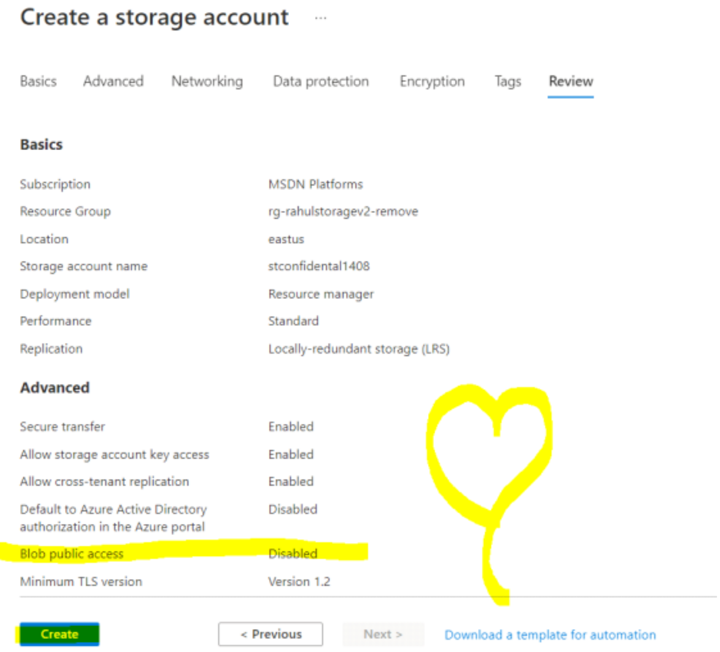
Create a storage account ···

Basics | Advanced | Networking | Data protection | **Encryption** | Tags | Review

Encryption type ⓘ *
● Microsoft-managed keys (MMK)
○ Customer-managed keys (CMK)

Enable support for customer-managed keys ⓘ
● Blobs and files only
○ All service types (blobs, files, tables, and queues)
⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ⓘ □



Create a storage account ···

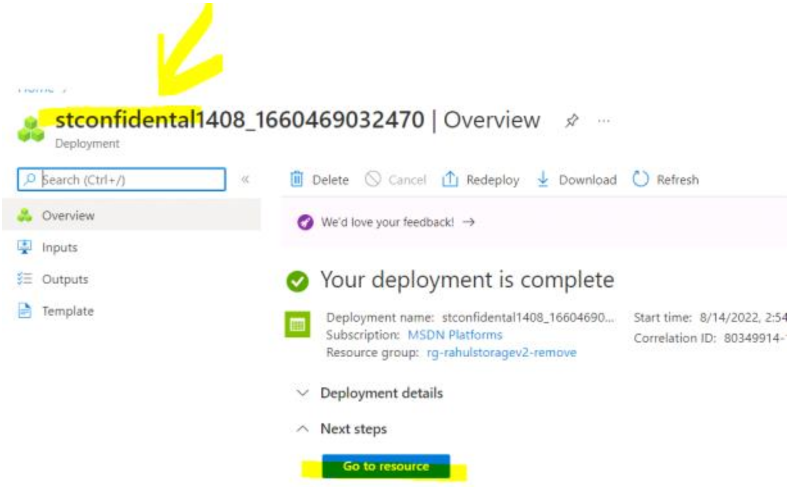
Basics | Advanced | Networking | Data protection | Encryption | Tags | **Review**

Basics

Subscription	MSDN Platforms
Resource Group	rg-rahulstoragev2-remove
Location	eastus
Storage account name	stconfidental1408
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Secure transfer	Enabled
Allow storage account key access	Enabled
Allow cross-tenant replication	Enabled
Default to Azure Active Directory authorization in the Azure portal	Disabled
Blob public access	Disabled
Minimum TLS version	Version 1.2



stconfidental1408_1660469032470 | Overview

Deployment

We'd love your feedback! →

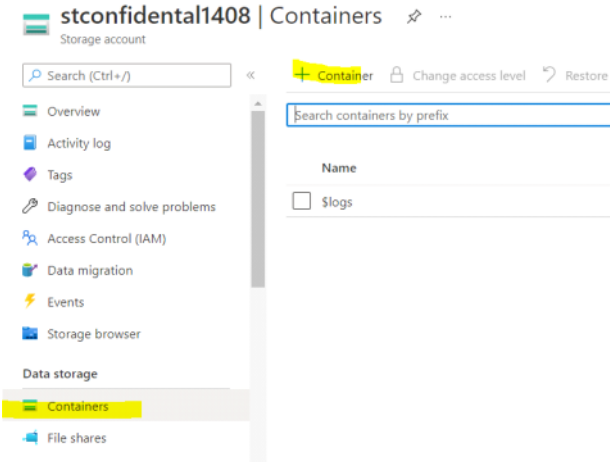
Your deployment is complete

Deployment name: stconfidental1408_16604690...
Subscription: MSDN Platforms
Resource group: rg-rahulstoragev2-remove

Start time: 8/14/2022, 2:54
Correlation ID: 80349914-

Deployment details

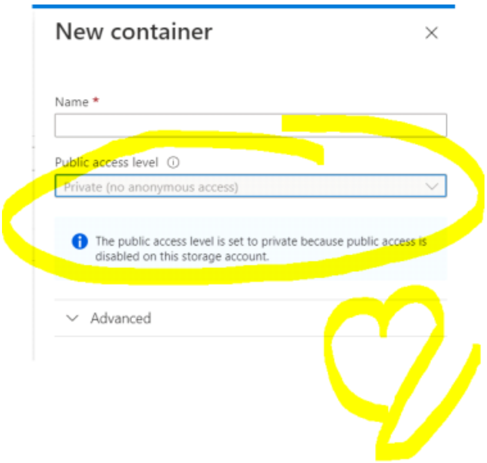
Next steps



stconfidental1408 | Containers

Storage account

	Name
□	$logs

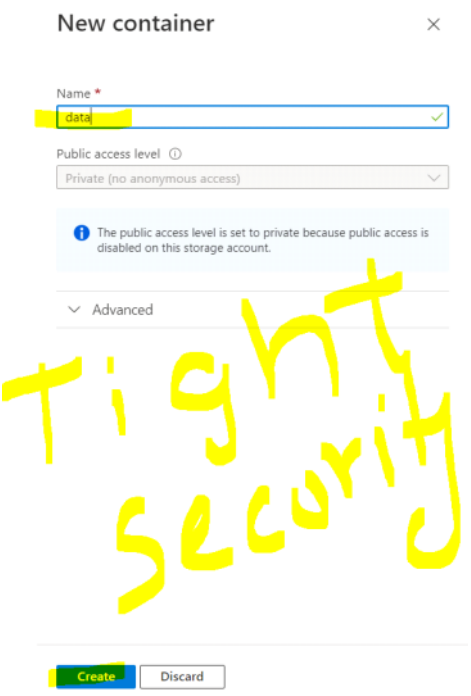


New container

Name *

Public access level: Private (no anonymous access)

The public access level is set to private because public access is disabled on this storage account.



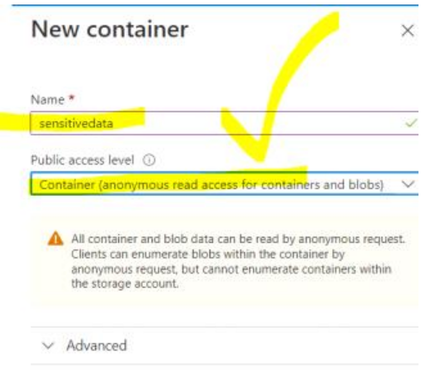
New container

Name * data

Public access level: Private (no anonymous access)

The public access level is set to private because public access is disabled on this storage account.

Mistakes can happen, like below

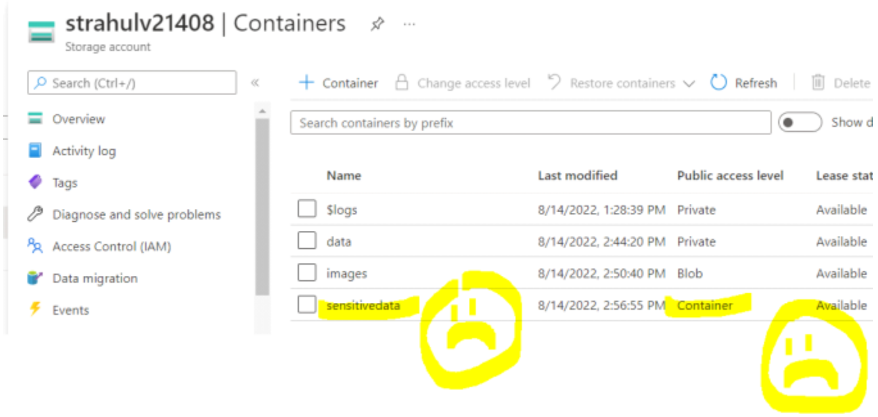


New container

Name * sensitivedata

Public access level: Container (anonymous read access for containers and blobs)

All container and blob data can be read by anonymous request. Clients can enumerate blobs within the container by anonymous request, but cannot enumerate containers within the storage account.

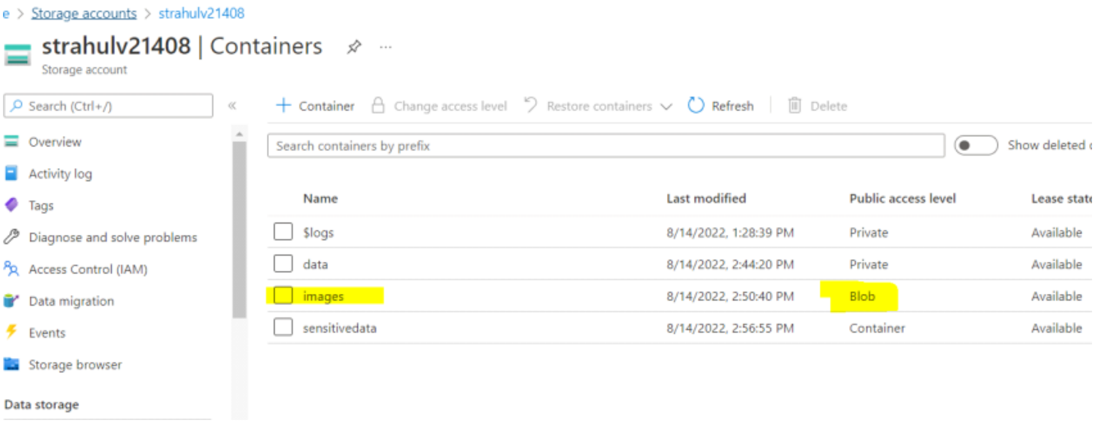


strahulv21408 | Containers

Storage account

Name	Last modified	Public access level	Lease stat
□ $logs	8/14/2022, 1:28:39 PM	Private	Available
□ data	8/14/2022, 2:44:20 PM	Private	Available
□ images	8/14/2022, 2:50:40 PM	Blob	Available
□ sensitivedata	8/14/2022, 2:56:55 PM	Container	Available

Let us now Upload a File into the Container

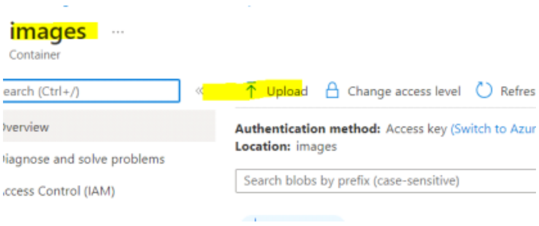


e > Storage accounts > strahulv21408

strahulv21408 | Containers

Storage account

	Name	Last modified	Public access level	Lease stat
□	$logs	8/14/2022, 1:28:39 PM	Private	Available
□	data	8/14/2022, 2:44:20 PM	Private	Available
□	images	8/14/2022, 2:50:40 PM	Blob	Available
□	sensitivedata	8/14/2022, 2:56:55 PM	Container	Available

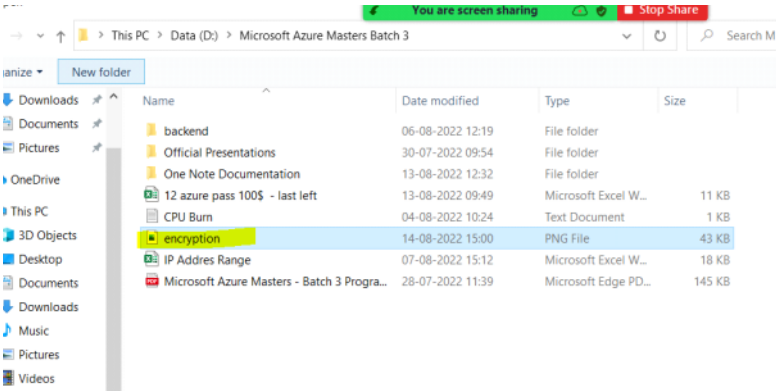


images

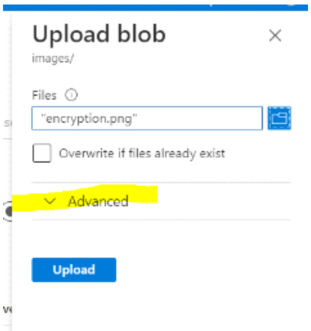
Container

Authentication method: Access key (Switch to Azur

Location: images



Name	Date modified	Type	Size
backend	06-08-2022 12:19	File folder	
Official Presentations	30-07-2022 09:54	File folder	
One Note Documentation	13-08-2022 12:32	File folder	
12 azure pass 100$ - last left	13-08-2022 09:49	Microsoft Excel W...	11 KB
CPU Burn	04-08-2022 10:24	Text Document	1 KB
encryption	14-08-2022 15:00	PNG File	43 KB
IP Addres Range	07-08-2022 15:12	Microsoft Excel W...	18 KB
Microsoft Azure Masters - Batch 3 Progra...	28-07-2022 11:39	Microsoft Edge PD...	145 KB

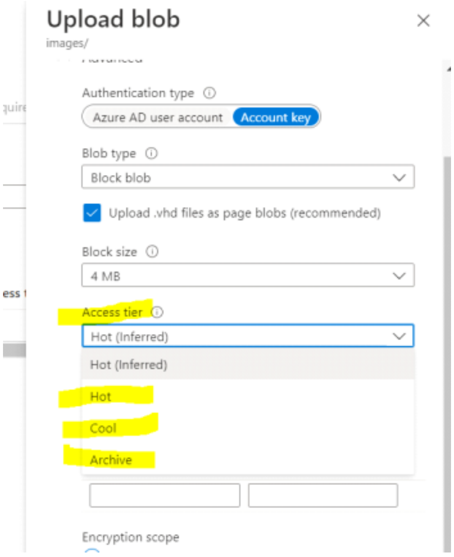


Upload blob

images/

Files: "encryption.png"

□ Overwrite if files already exist



Upload blob

images/

Authentication type ⓘ

Azure AD user account | **Account key**

Blob type ⓘ

Block blob

☑ Upload .vhd files as page blobs (recommended)

Block size ⓘ

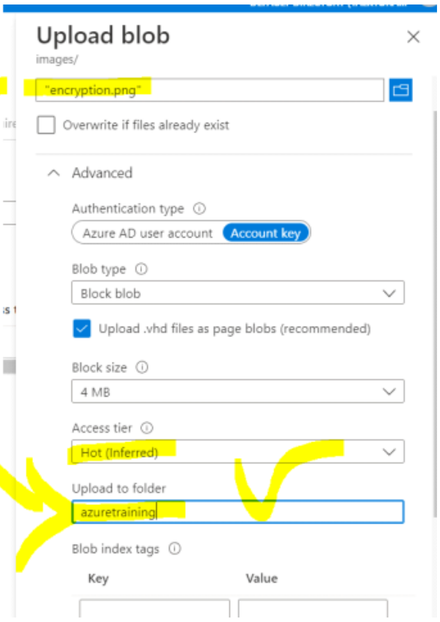
4 MB

Access tier ⓘ

Hot (Inferred)

- Hot (Inferred)
- Hot
- Cool
- Archive

Encryption scope



Upload blob

images/

"encryption.png"

□ Overwrite if files already exist

Advanced

Authentication type ⓘ

Azure AD user account | **Account key**

Blob type ⓘ

Block blob

☑ Upload .vhd files as page blobs (recommended)

Block size ⓘ

4 MB

Access tier ⓘ

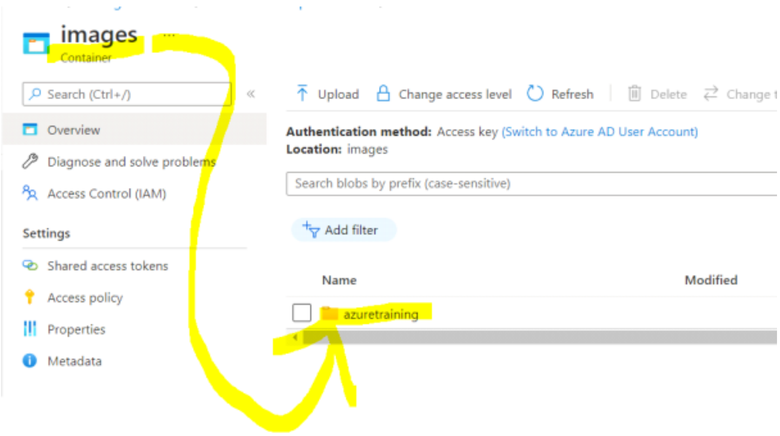
Hot (Inferred)

Upload to folder

azuretraining

Blob index tags ⓘ

Key	Value



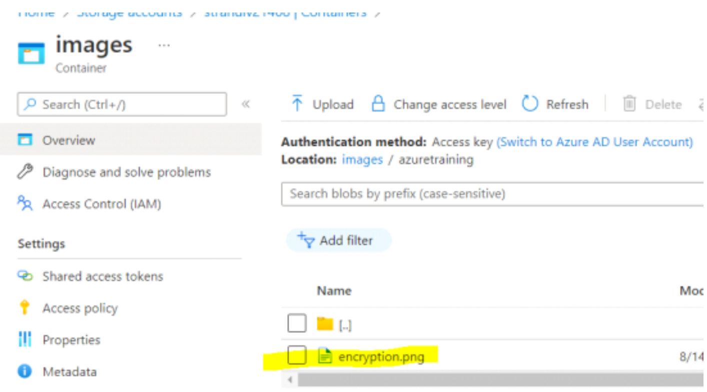
images

Container

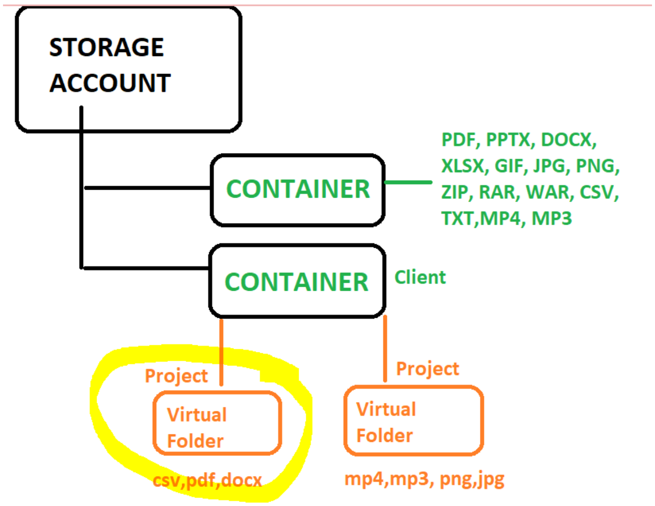
Authentication method: Access key (Switch to Azure AD User Account)
Location: images

Search blobs by prefix (case-sensitive)

Name	Modified
□ azuretraining	



Authentication method: Access key (Switch to Azure AD User Account)
Location: images / azuretraining



STORAGE ACCOUNT

CONTAINER

PDF, PPTX, DOCX, XLSX, GIF, JPG, PNG, ZIP, RAR, WAR, CSV, TXT,MP4, MP3

CONTAINER

Client

Project

Virtual Folder

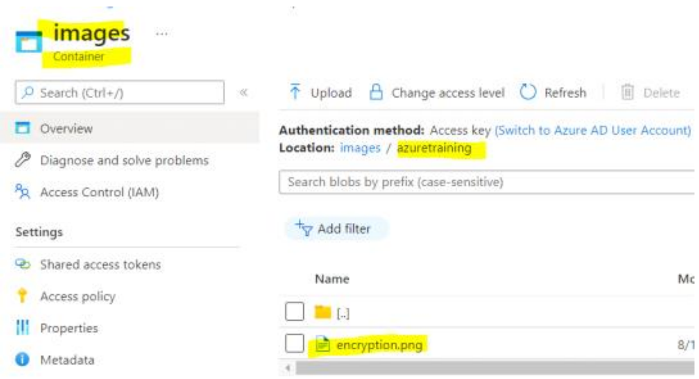
csv,pdf,docx

Project

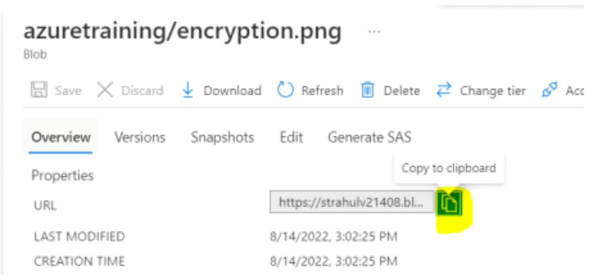
Virtual Folder

mp4,mp3, png,jpg

Can we see the image uploaded from the browser



Authentication method: Access key (Switch to Azure AD User Account)
Location: images / azuretraining



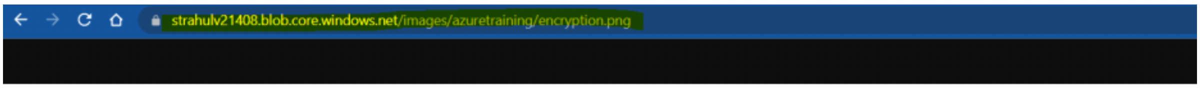
Properties

URL https://strahulv21408.bl...

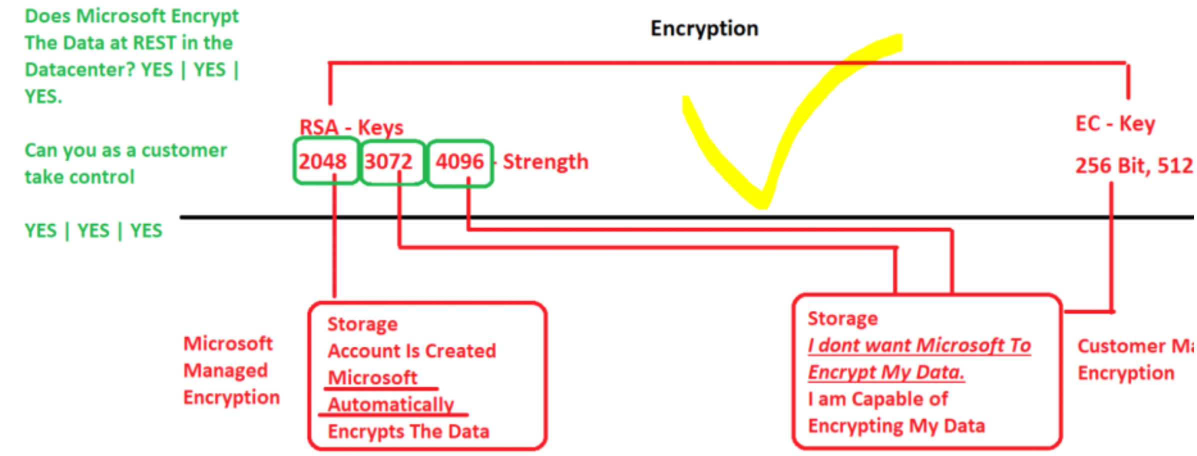
LAST MODIFIED 8/14/2022, 3:02:25 PM

CREATION TIME 8/14/2022, 3:02:25 PM

https://strahulv21408.blob.core.windows.net/images/azuretraining/encryption.png



strahulv21408.blob.core.windows.net/images/azuretraining/encryption.png



Does Microsoft Encrypt The Data at REST in the Datacenter? YES | YES | YES.

Can you as a customer take control

YES | YES | YES

Encryption

RSA - Keys

2048 3072 4096 Strength

EC - Key

256 Bit, 512

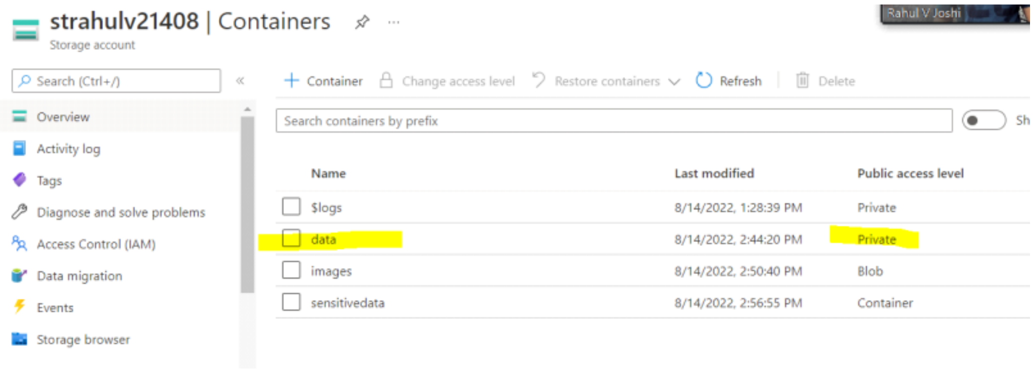
Microsoft Managed Encryption

Storage Account Is Created Microsoft Automatically Encrypts The Data

Storage *I dont want Microsoft To Encrypt My Data.* I am Capable of Encrypting My Data

Customer M Encryption

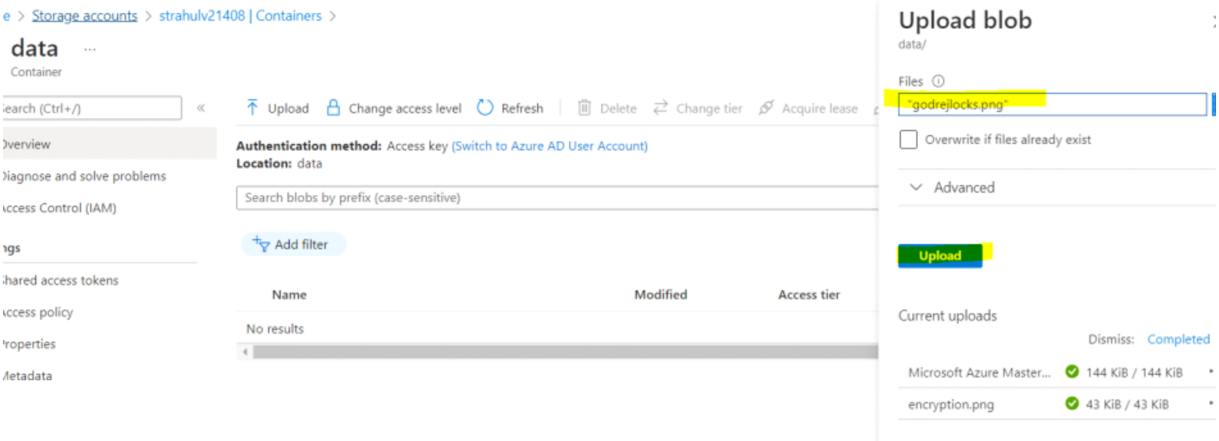
Now, we upload to Private Container, which is not Public



strahulv21408 | Containers

Storage account

Name	Last modified	Public access level
$logs	8/14/2022, 1:28:39 PM	Private
data	8/14/2022, 2:44:20 PM	Private
images	8/14/2022, 2:50:40 PM	Blob
sensitivedata	8/14/2022, 2:56:55 PM	Container



e > Storage accounts > strahulv21408 | Containers >

data

Container

Authentication method: Access key (Switch to Azure AD User Account)
Location: data

Search blobs by prefix (case-sensitive)

Name	Modified	Access tier
No results		

Upload blob

data/

Files: "godrejlocks.png"

□ Overwrite if files already exist

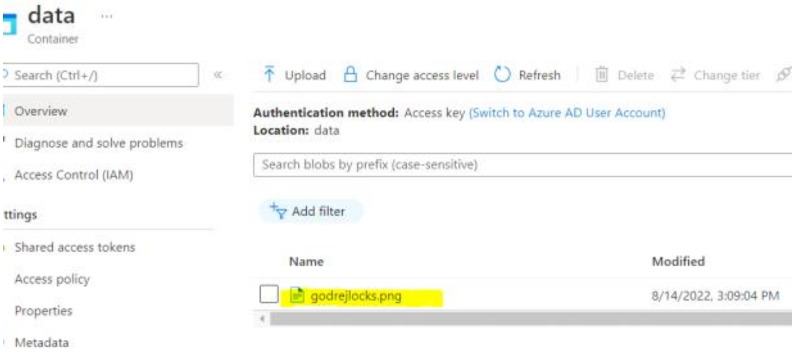
Advanced

Upload

Current uploads

Dismiss: Completed

Microsoft Azure Master...	✓ 144 KiB / 144 KiB
encryption.png	✓ 43 KiB / 43 KiB



data ···
Container

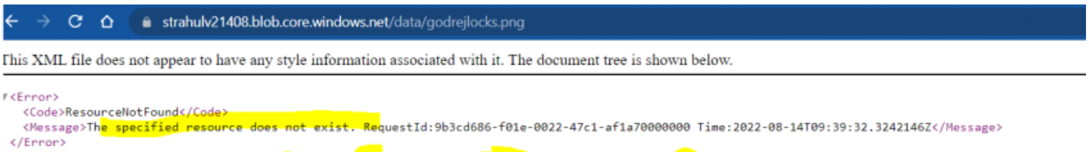
Search (Ctrl+/)

Authentication method: Access key (Switch to Azure AD User Account)
Location: data

Search blobs by prefix (case-sensitive)

	Name	Modified
□	godrejlocks.png	8/14/2022, 3:09:04 PM

https://strahulv21408.blob.core.windows.net/data/godrejlocks.png

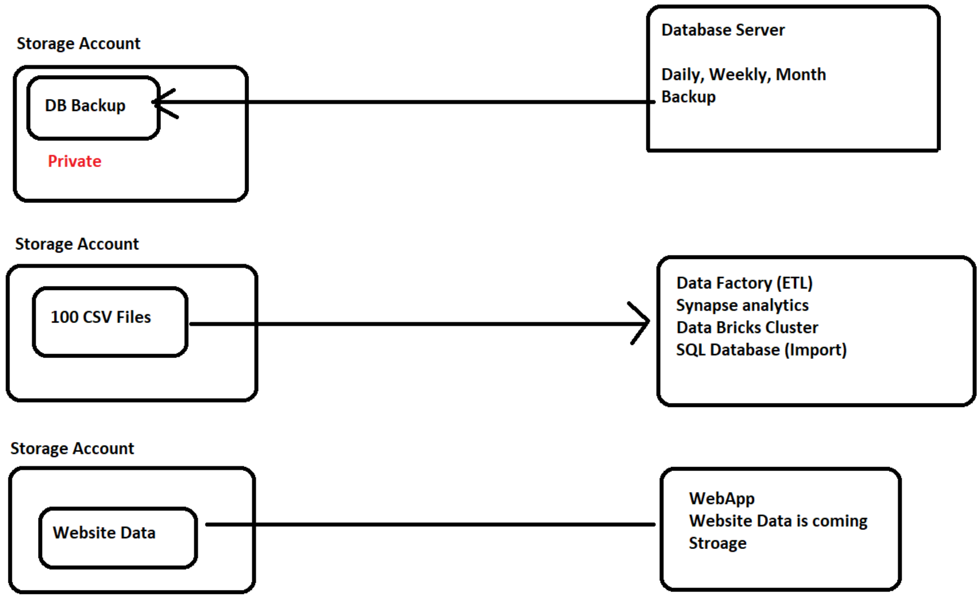


strahulv21408.blob.core.windows.net/data/godrejlocks.png

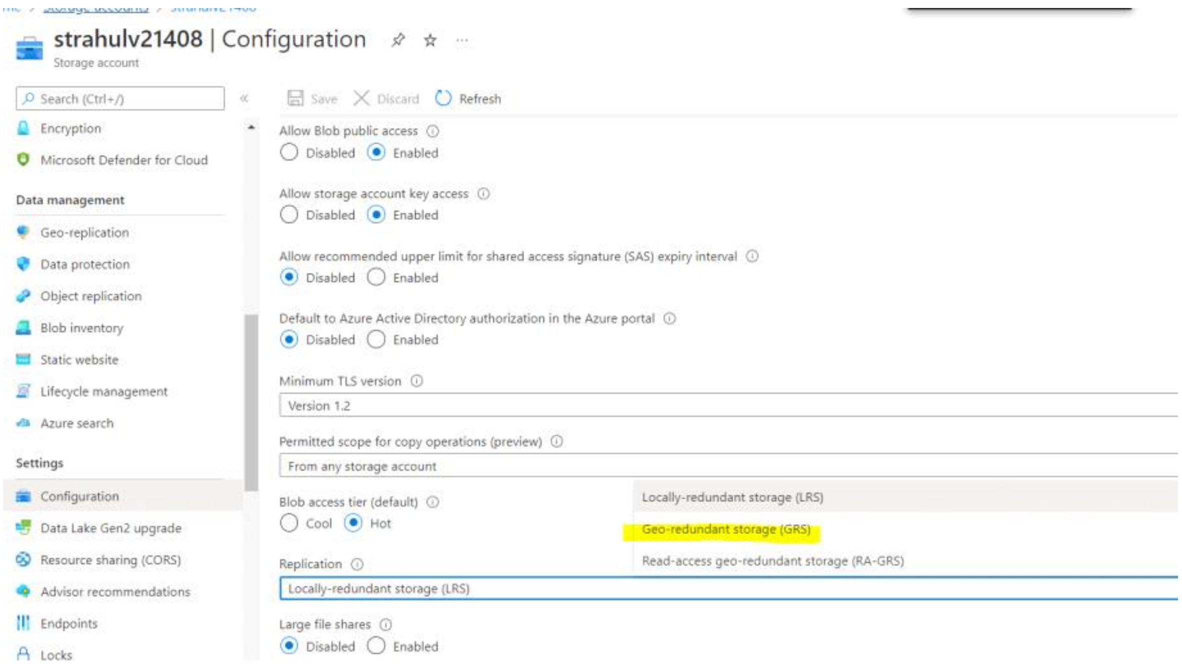
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
  <Code>ResourceNotFound</Code>
  <Message>The specified resource does not exist. RequestId:9b3cd686-f01e-0022-47c1-af1a70000000 Time:2022-08-14T09:39:32.3242146Z</Message>
</Error>
```

Private ☺ ☺



Action 2: The customer mentions that, by default they choose LRS as Redundancy, so they need to configure GRS as that was change as a decision.


strahulv21408 | Configuration
Storage account

Allow Blob public access: ○ Disabled ● Enabled

Allow storage account key access: ○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval: ● Disabled ○ Enabled

Default to Azure Active Directory authorization in the Azure portal: ● Disabled ○ Enabled

Minimum TLS version: Version 1.2

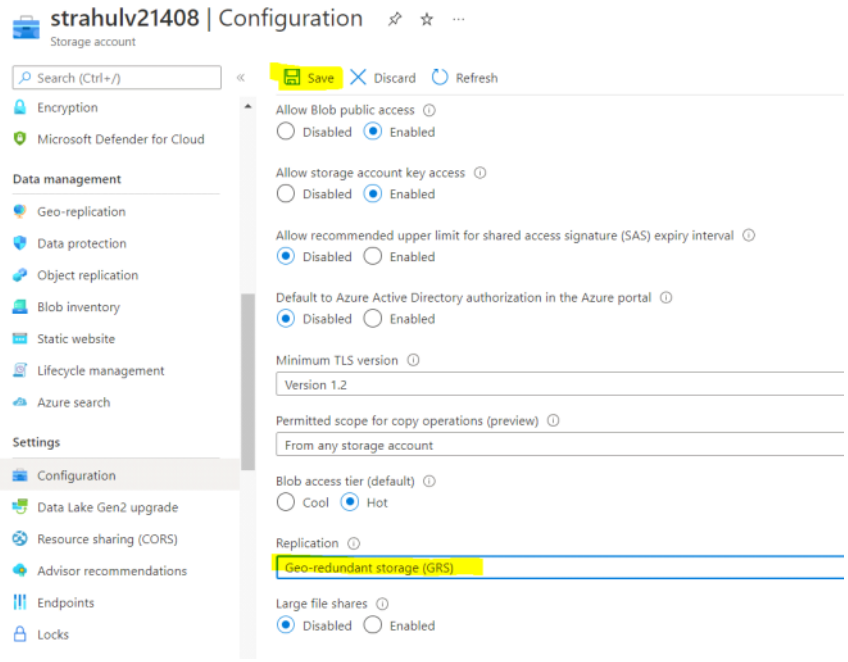
Permitted scope for copy operations (preview): From any storage account

Blob access tier (default): ○ Cool ● Hot

Replication: Locally-redundant storage (LRS)
- Locally-redundant storage (LRS)
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)

Large file shares: ● Disabled ○ Enabled

You can see above, that ZRS - Zone Redundant Storage is not there. Which means, ZRS can only be used during creation of storage, not after storage is created.


strahulv21408 | Configuration
Storage account

Allow Blob public access: ○ Disabled ● Enabled

Allow storage account key access: ○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval: ● Disabled ○ Enabled

Default to Azure Active Directory authorization in the Azure portal: ● Disabled ○ Enabled

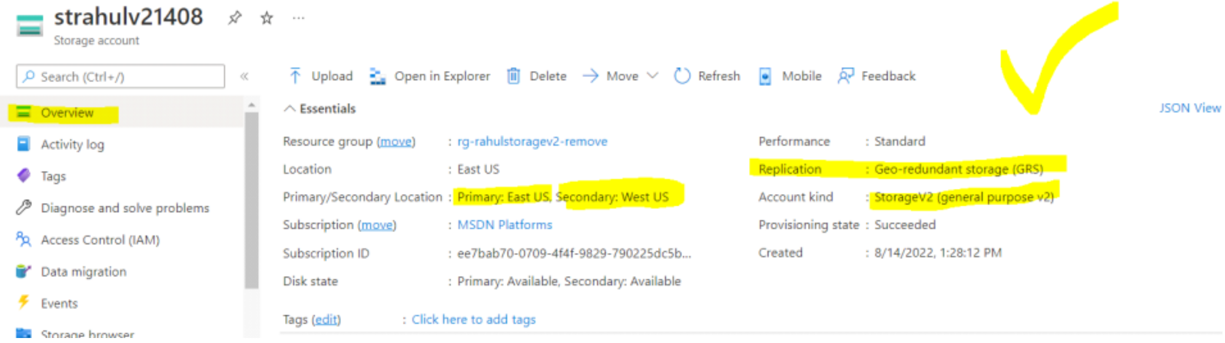
Minimum TLS version: Version 1.2

Permitted scope for copy operations (preview): From any storage account

Blob access tier (default): ○ Cool ● Hot

Replication: Geo-redundant storage (GRS)

Large file shares: ● Disabled ○ Enabled


strahulv21408
Storage account

Resource group (move)	: rg-rahulstoragev2-remove	Performance	: Standard
Location	: East US	Replication	: Geo-redundant storage (GRS)
Primary/Secondary Location	: Primary: East US, Secondary: West US	Account kind	: StorageV2 (general purpose v2)
Subscription (move)	: MSDN Platforms	Provisioning state	: Succeeded
Subscription ID	: ee7bab70-0709-4f4f-9829-790225dc5b...	Created	: 8/14/2022, 1:28:12 PM
Disk state	: Primary: Available, Secondary: Available		
Tags (edit)	: Click here to add tags		

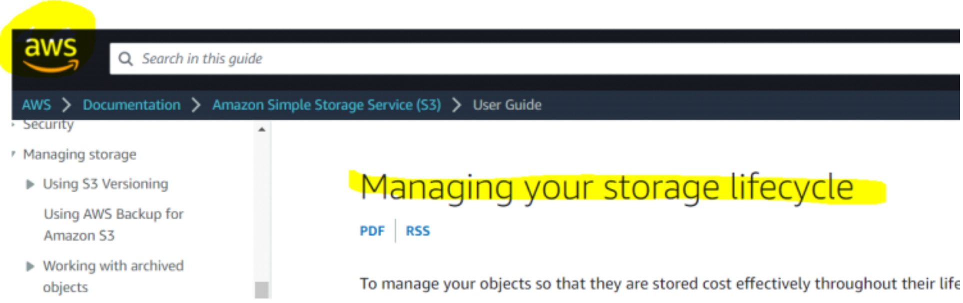
Primary - East US, Secondary - West US, Microsoft did not give you choice to select the region

Action 3:

The customer also mentions that After 30 days the file is last modified, the access tier should change to Cool and after 60 days from the last modified the Access tier should change to Archive and after 365 days, the file should be deleted. This should be done automatically.

Imagine, you have 10000 files, it be next to impossible to manually move from Hot To Cool, Cool to Archive and delete if required.

Life Cycle Management



aws Search in this guide

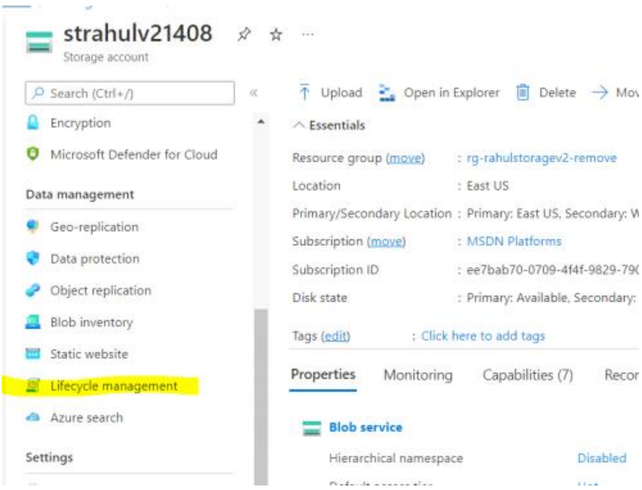
AWS > Documentation > Amazon Simple Storage Service (S3) > User Guide

Security
Managing storage
Using S3 Versioning
Using AWS Backup for Amazon S3
Working with archived objects

Managing your storage lifecycle

PDF | RSS

To manage your objects so that they are stored cost effectively throughout their life



strahulv21408

Storage account

Search (Ctrl+/)

Encryption
Microsoft Defender for Cloud

Data management

Geo-replication
Data protection
Object replication
Blob inventory
Static website
Lifecycle management
Azure search

Settings

Upload | Open in Explorer | Delete | Mov

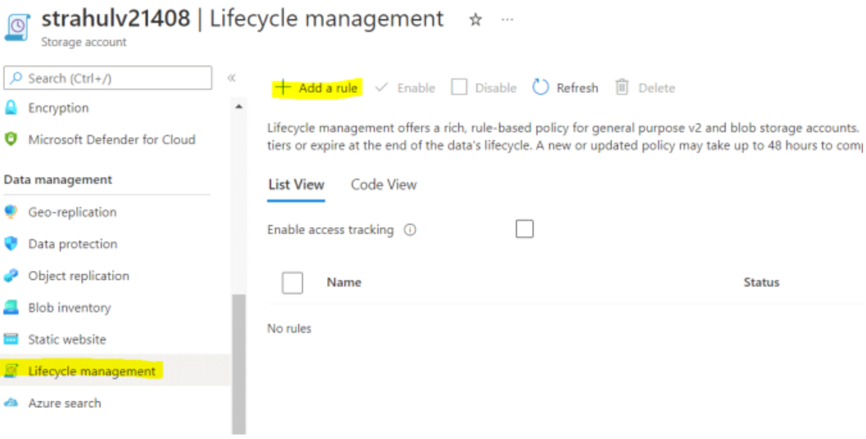
Essentials

Resource group (move) : rg-rahulstoragev2-remove
Location : East US
Primary/Secondary Location : Primary: East US, Secondary: W
Subscription (move) : MSDN Platforms
Subscription ID : ee7bab70-0709-4f4f-9829-79(
Disk state : Primary: Available, Secondary:
Tags (edit) : Click here to add tags

Properties | Monitoring | Capabilities (7) | Recor

Blob service
Hierarchical namespace Disabled

EXAM Question



strahulv21408 | Lifecycle management

Storage account

Search (Ctrl+/)

Encryption
Microsoft Defender for Cloud

Data management

Geo-replication
Data protection
Object replication
Blob inventory
Static website
Lifecycle management
Azure search

+ Add a rule | Enable | Disable | Refresh | Delete

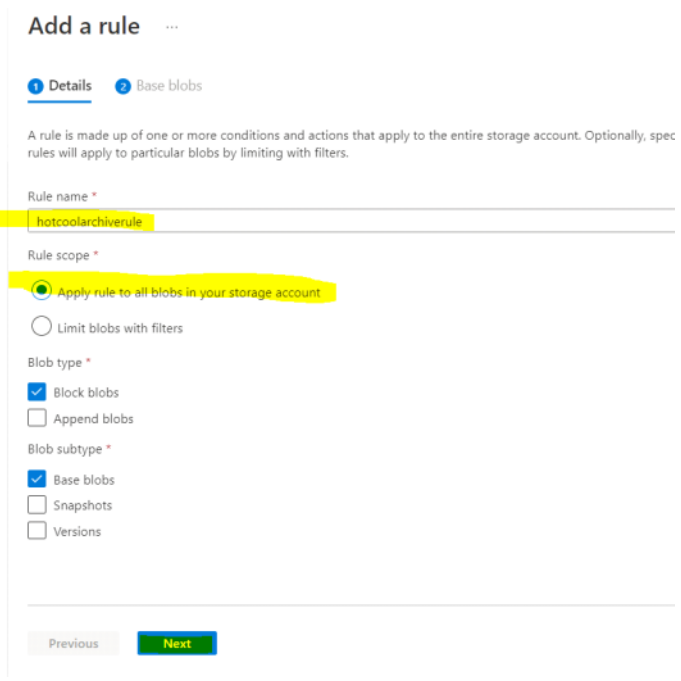
Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. tiers or expire at the end of the data's lifecycle. A new or updated policy may take up to 48 hours to com

List View | Code View

Enable access tracking ⓘ □

□ Name Status

No rules



Add a rule ···

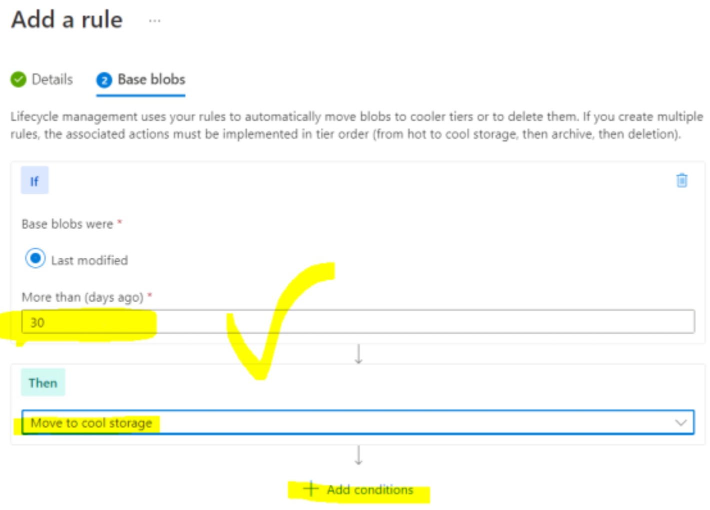
A rule is made up of one or more conditions and actions that apply to the entire storage account. Optionally, spec rules will apply to particular blobs by limiting with filters.

Rule name *
hotcoolarchiverule

Rule scope *
● Apply rule to all blobs in your storage account
○ Limit blobs with filters

Blob type *
☑ Block blobs
□ Append blobs

Blob subtype *
☑ Base blobs
□ Snapshots
□ Versions



Add a rule ···

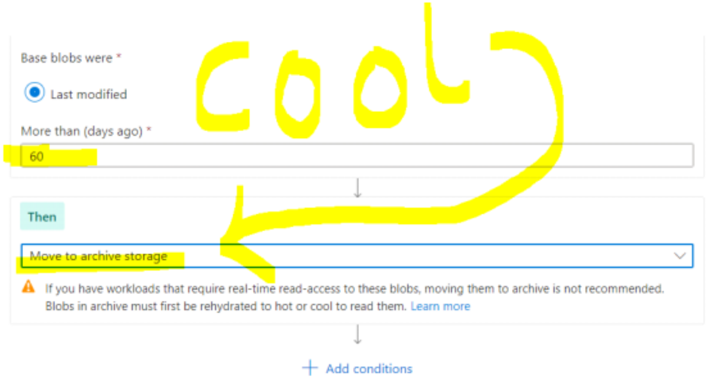
Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *
● Last modified

More than (days ago) *
30

Then
Move to cool storage



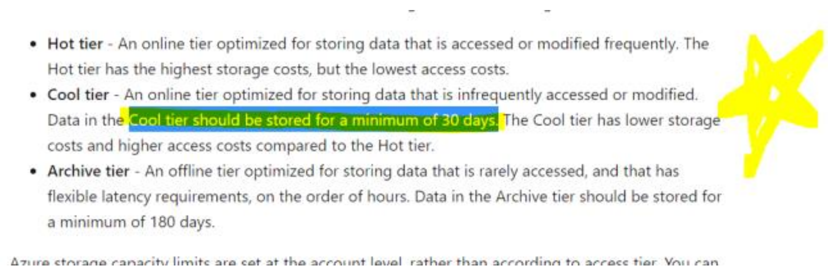
cool

Base blobs were *
● Last modified

More than (days ago) *
60

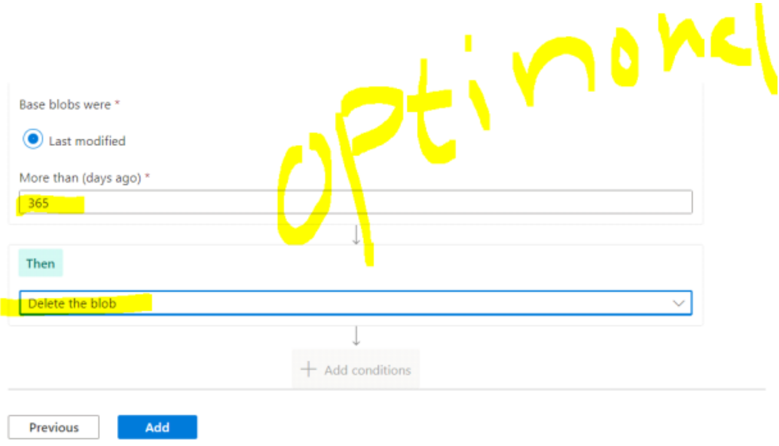
Then
Move to archive storage

⚠ If you have workloads that require real-time read-access to these blobs, moving them to archive is not recommended. Blobs in archive must first be rehydrated to hot or cool to read them. Learn more



- **Hot tier** - An online tier optimized for storing data that is accessed or modified frequently. The Hot tier has the highest storage costs, but the lowest access costs.
- **Cool tier** - An online tier optimized for storing data that is infrequently accessed or modified. Data in the Cool tier should be stored for a minimum of 30 days. The Cool tier has lower storage costs and higher access costs compared to the Hot tier.
- **Archive tier** - An offline tier optimized for storing data that is rarely accessed, and that has flexible latency requirements, on the order of hours. Data in the Archive tier should be stored for a minimum of 180 days.

Azure storage capacity limits are set at the account level, rather than according to access tier. You can



Base blobs were *

● Last modified

More than (days ago) *

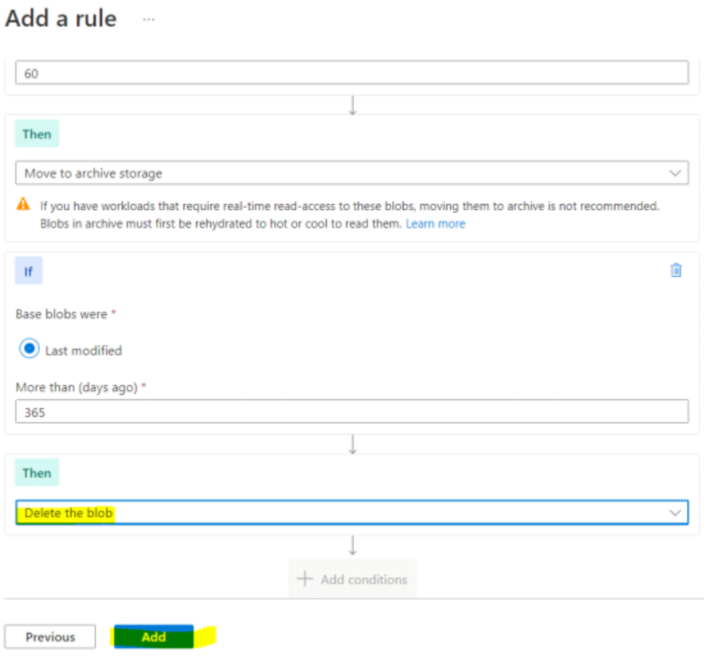
365

Then

Delete the blob

In Archive, the file should stay for 180 days, then only early deletion charges are not applied

But, Delete is optional. You cannot force anyone to delete after any number of dats



Add a rule ···

60

Then

Move to archive storage

⚠ If you have workloads that require real-time read-access to these blobs, moving them to archive is not recommended. Blobs in archive must first be rehydrated to hot or cool to read them. Learn more

If

Base blobs were *

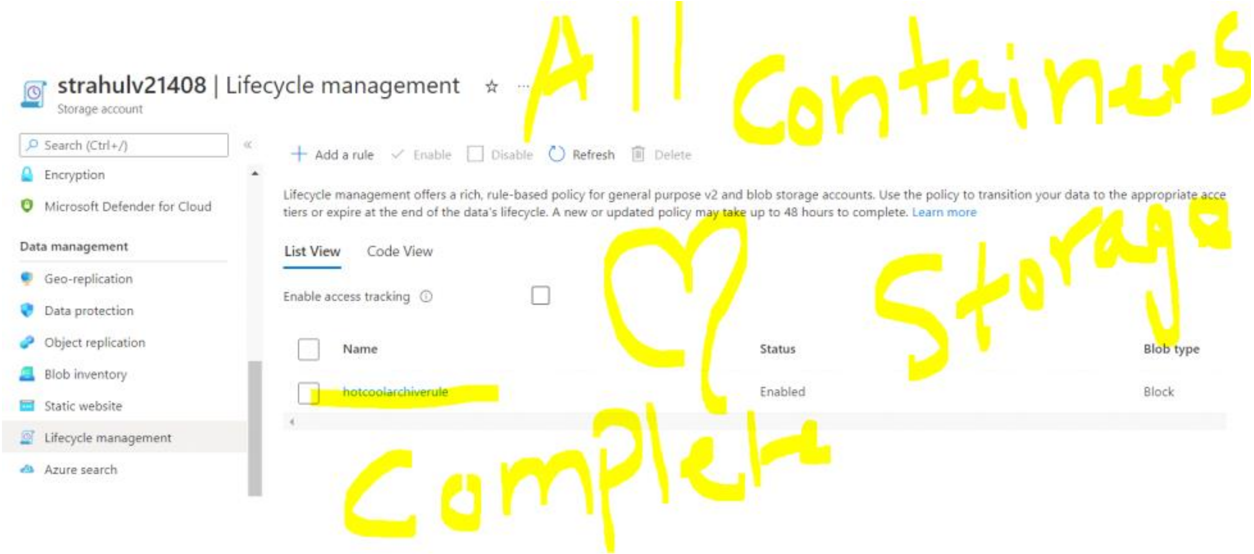
● Last modified

More than (days ago) *

365

Then

Delete the blob



strahulv21408 | Lifecycle management ☆ ···

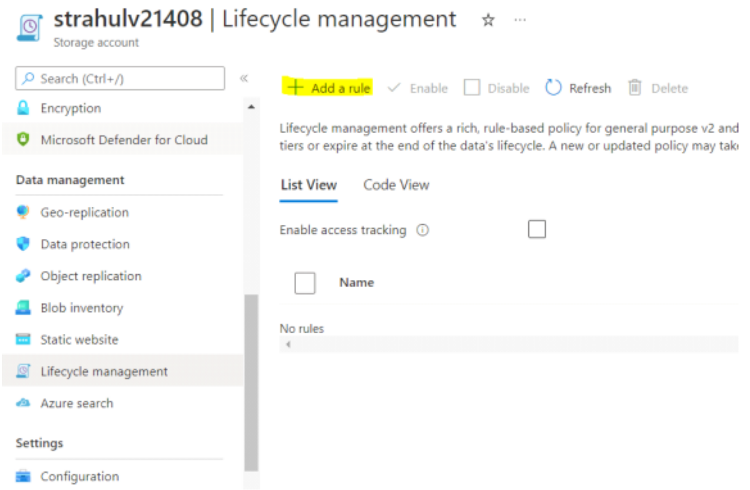
Storage account

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to the appropriate acce tiers or expire at the end of the data's lifecycle. A new or updated policy may take up to 48 hours to complete. Learn more

Enable access tracking ⓘ □

□	Name	Status	Blob type
□	hotcoolarchiverule	Enabled	Block

Can we specify these rules for only Specific container?



strahulv21408 | Lifecycle management ☆ ···

Storage account

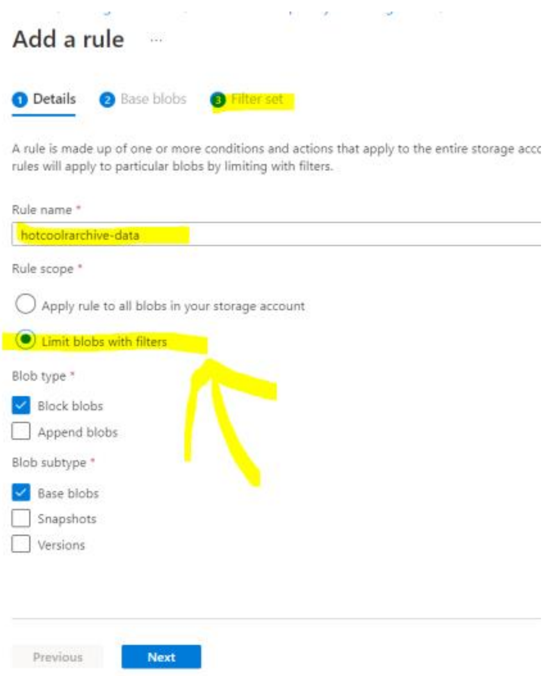
Lifecycle management offers a rich, rule-based policy for general purpose v2 and tiers or expire at the end of the data's lifecycle. A new or updated policy may tak

List View | Code View

Enable access tracking ⓘ □

□ Name

No rules



Add a rule ···

A rule is made up of one or more conditions and actions that apply to the entire storage accc rules will apply to particular blobs by limiting with filters.

Rule name *

hotcoolrarchive-data

Rule scope *

○ Apply rule to all blobs in your storage account

● Limit blobs with filters

Blob type *

☑ Block blobs

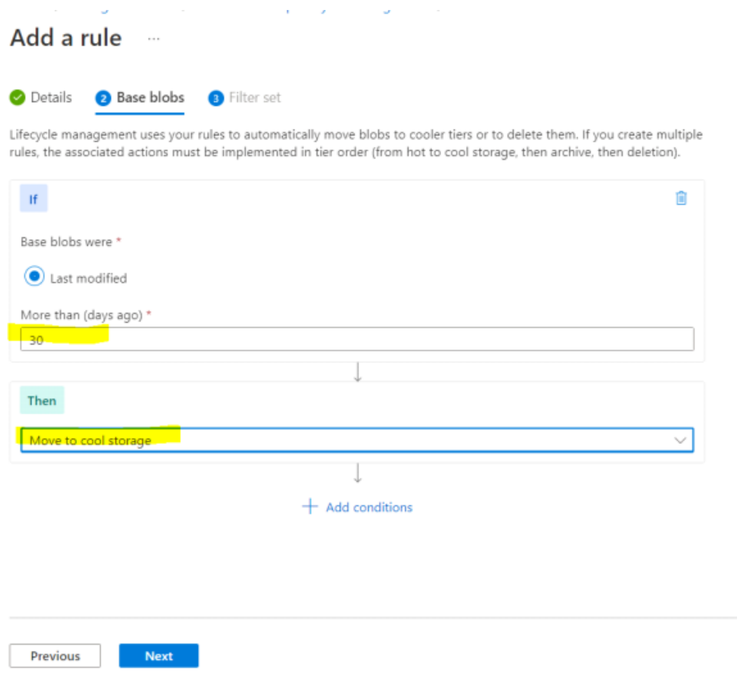
□ Append blobs

Blob subtype *

☑ Base blobs

□ Snapshots

□ Versions



Add a rule ···

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *

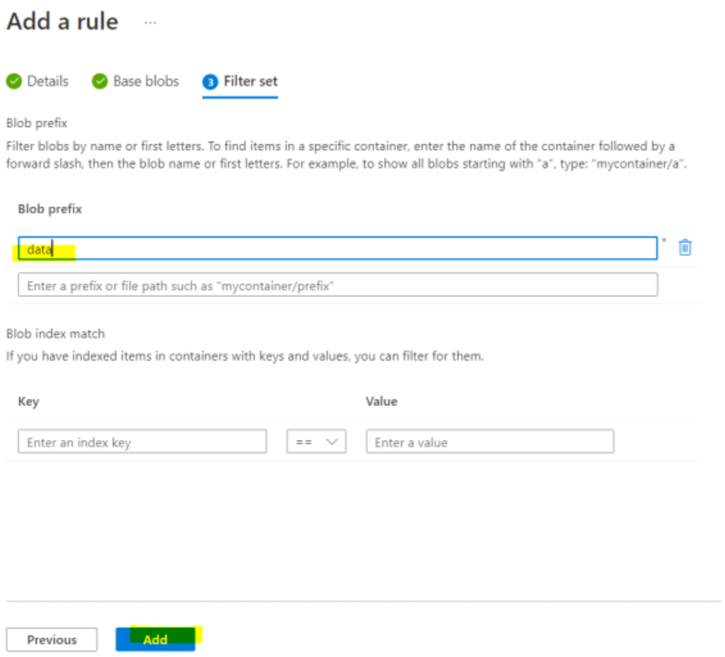
● Last modified

More than (days ago) *

30

Then

Move to cool storage



Blob prefix

Filter blobs by name or first letters. To find items in a specific container, enter the name of the container followed by a forward slash, then the blob name or first letters. For example, to show all blobs starting with "a", type: "mycontainer/a".

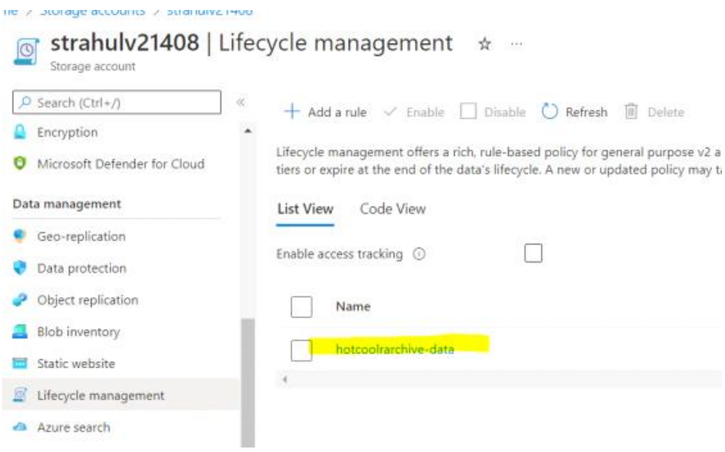
Blob prefix: data

Enter a prefix or file path such as "mycontainer/prefix"

Blob index match

If you have indexed items in containers with keys and values, you can filter for them.

Key		Value
Enter an index key	==	Enter a value



Lifecycle management offers a rich, rule-based policy for general purpose v2 a tiers or expire at the end of the data's lifecycle. A new or updated policy may t

Enable access tracking ⓘ □

□	Name
□	hotcoolrarchive-data

This means, this logic now only applies to data container, from this container after 30 days, files be changed from Hot To Co ol, other containers will not have any impact and will stay as HOT, unless you change it.

End of Day 5