A decorative pattern of hexagons in various shades of blue and black is located in the top left corner of the page. The hexagons are arranged in a grid-like pattern, with some being solid colors and others having a lighter, semi-transparent appearance.

RSTOR Space and Rubrik

Configuring RSTOR Space as a Rubrik Archive

November 2020

Prepared by: RSTOR Support

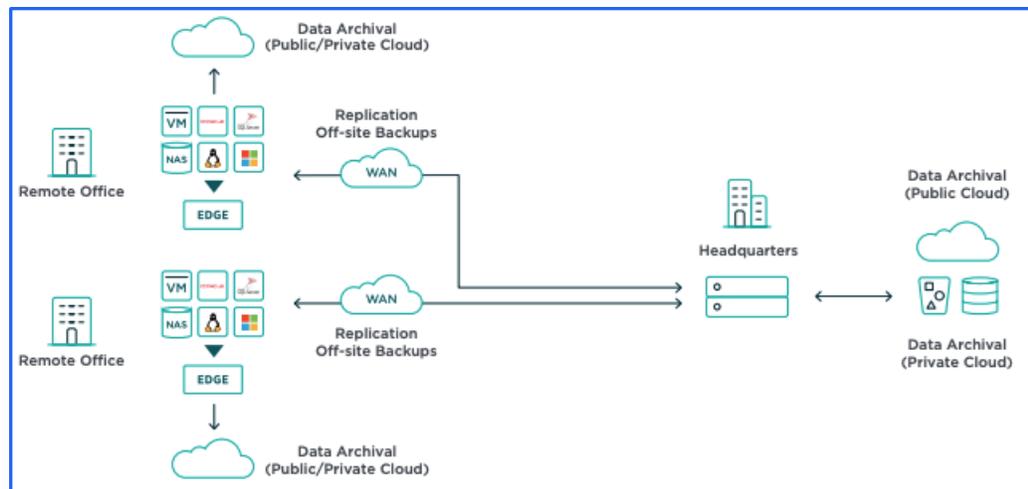
Table of Contents

1	Rubrik Components.....	3
2	Amazon S3 Compatible Object Storage	4
2.1	Instant Archiving Note	9

1 Rubrik Components

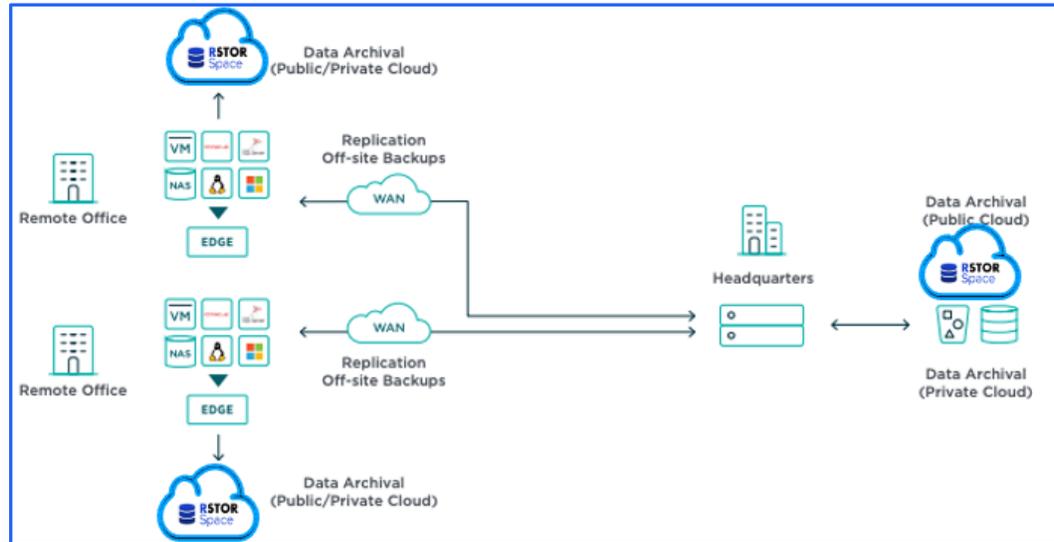
Rubrik is a Cloud Data Management Platform that can run on-prem and in public clouds. Rubrik is a single platform that converges the components of backup software and backup infrastructure such as servers, deduplicating storage, and long-term retention data in a simple, scalable fashion. It indexes and manages all data in the cloud, at the edge, or on-prem for backup, disaster recovery, archival, compliance, analytics, and copy data management. Rubrik powers on data instantly (for recovery or for test and development).

The benefits of Rubrik include simplified backup and recovery, accelerated cloud adoption, and the ability to automate at scale.



2 Amazon S3 Compatible Object Storage

Complete the following steps to add RSTOR Space as an archive for Rubrik.



1. Create an RSTOR user. Navigate to the “Users” tab and click on the “plus” icon in the upper right-hand corner to create a new user.
2. Once completed, generate an access key by clicking on the new email and clicking “+ GENERATE KEY”. Take note of this information because it will not be displayed again.
3. Navigate to the “Buckets” tab and create an RSTOR bucket. The naming convention for buckets to be used as Rubrik Archives is:

<prefix>-rubrik-<number> e.g. rstor-rubrik-0 (see name in screenshot below)

<number> starts at 0 and the **<prefix>** used here must also be used when attaching the archive in step 8. It’s possible to use multiple buckets when adding the archive, but just one is fine.

Add new bucket

Choose a name for new bucket, the replication policy and whether the bucket will be public or not.

Name of the bucket *

rstor-rubrik-0

Bucket name must be globally unique. Between 3 - 63 chars. Lowercase letters, digits and - allowed. Must start with a char. 14 / 63

Regions

Select the region(s) where you want the bucket to be created and replicated.

us-east-1 us-central-1 us-west-1

Access Mode

Private

Versioning

Keep previous versions of objects when they are overwritten or deleted.

Enabled Disabled

Object Locking

Store objects using a write-once-read-many (WORM) model to meet regulatory requirements or add an extra layer of protection against object changes and deletion.

Will enable versioning automatically.

Enabled Disabled

**Note: Rubrik is not version aware so versioning should be disabled*

- Navigate to the "Policies" tab and add a Rubrik policy to the RSTOR bucket we just created. See the screenshot below.

RSTOR Buckets Users **Policies** Objects Roles Support

Policies > New Policy

Policy Name: rubrik 6 / 25

Policy name can contain only letters, numbers, and -

Policy Description: rubrik policy 14 / 50

Policy description will be displayed on the Rubrik console.

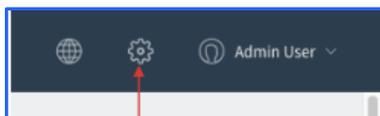
Add permissions on

Select bucket(s)

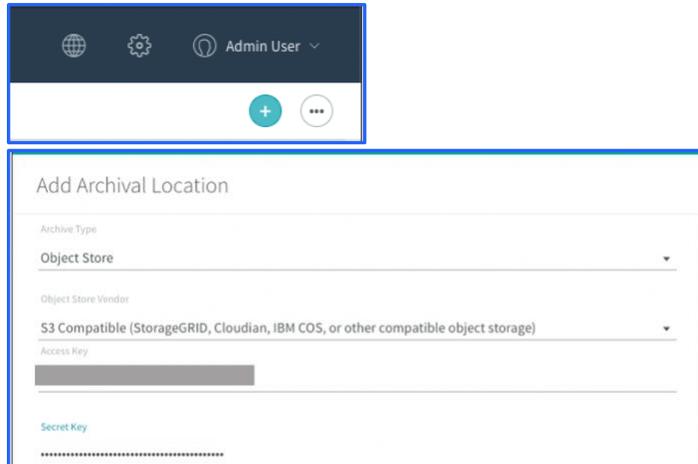
The policy will be enforced on the selected buckets. Choose "All buckets" to make the policy global.

Bucket	Read	Write	List	Delete	Actions
rstor-rubrik-0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="⋮"/>

- Using Chrome, connect to any of the IP addresses of the Rubrik Cluster. Login to Rubrik using an admin account.



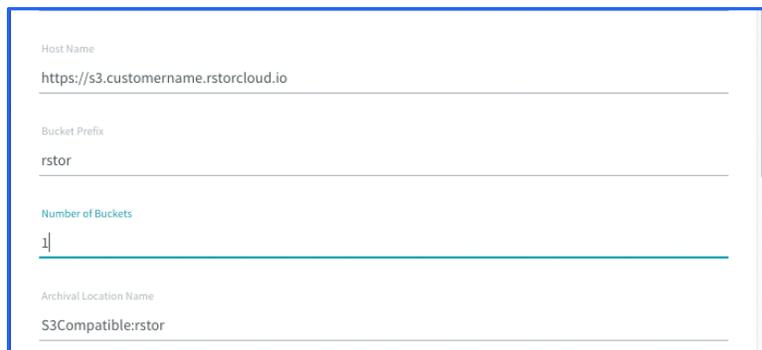
- Click on the “gear” icon in the top right of the GUI and click on “Archival Locations” in the dropdown menu under “System Configuration”.
- Click on the “+” icon to add an archival location. For “Archive Type” choose “Object Store”. For “Object Store Vendor” choose “S3 Compatible”. Enter your previously generated RSTOR access key and secret key that were created in step 2.



- Enter the RSTOR customer’s host name. The bucket prefix has to match the prefix used when creating the bucket in RSTOR back in step 3. You may edit the default Archival Location Name if you wish. Rubrik encrypts the data stored in the Cloud Archive using customer created RSA keys using a secure computer that has the OpenSSL toolkit.

“openssl genrsa -out rubrik_encryption_key.pem 2048”

The customer needs to keep the RSA key safe to connect to the archive from another Rubrik Cluster for DR purposes.



- Select “Enable Archive Consolidation”.

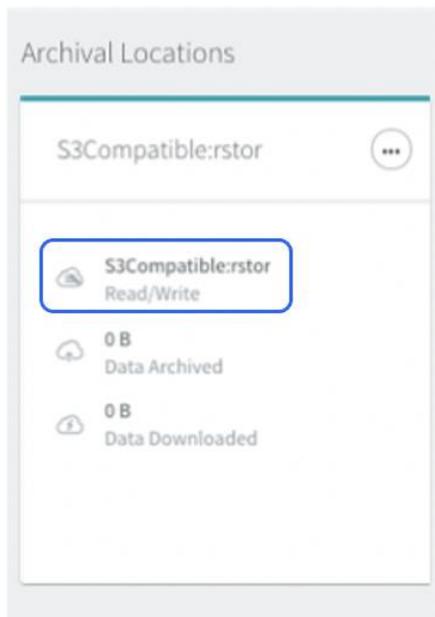
Enable Archive Consolidation

When Archival Consolidation is enabled, Rubrik merges the expired set of snapshots with the next live snapshot. This reduces storage requirements and reduces the snapshot chain length. With reduced snapshot chain length, a full snapshot is only required for the first snapshot and subsequent snapshots use incremental-forever snapshots.

Even though the capacity required for the archive is reduced, the Rubrik Cluster will carry out more I/O against the Archive.

10. Click “Add” and Rubrik will now attempt to connect to the Archive.

The Rubrik GUI will now revert back to the Archive Overview page and the Archival status will report as “Connecting” for a short period of time. Once connected, its verified that Rubrik has the required Read/Write access, and the status will change.



11. Now, to create Rubrik SLA's that use the Archive, in the left-hand side of the Rubrik GUI, click on “Local Domains” under SLA's.
12. Click on the “+” icon in the top-right of the Rubrik GUI.
13. Enter an SLA name. Provide information about the frequency of the snapshots and the retention period for each type of snapshot. Once inputted, click “Next”.

In this example, snapshots are taken every 1 hour and kept for 3 days. Daily snapshots are taken every 1 day and kept for 30 days. Monthly snapshots are taken and kept for 12 months. Yearly snapshots are taken and kept for 7 years.

Create SLA Domain

1 Set Frequency and Retention 2 Set Archiving and Replication (Optional) 3 Summary

SLA Domain Name
RSTOR SLA

Continuous Data Protection

Service Level Agreement
Choose how often we take snapshots and the length of time we keep them.

Weekly and Quarterly Frequencies

Take Snapshots:	Keep Snapshots:
Every (Hours) 1	For (Days) 3
Every (Days) 1	For (Days) 30
Every (Months) 1	For (Months) 12
Every (Years) 1	For (Years) 7

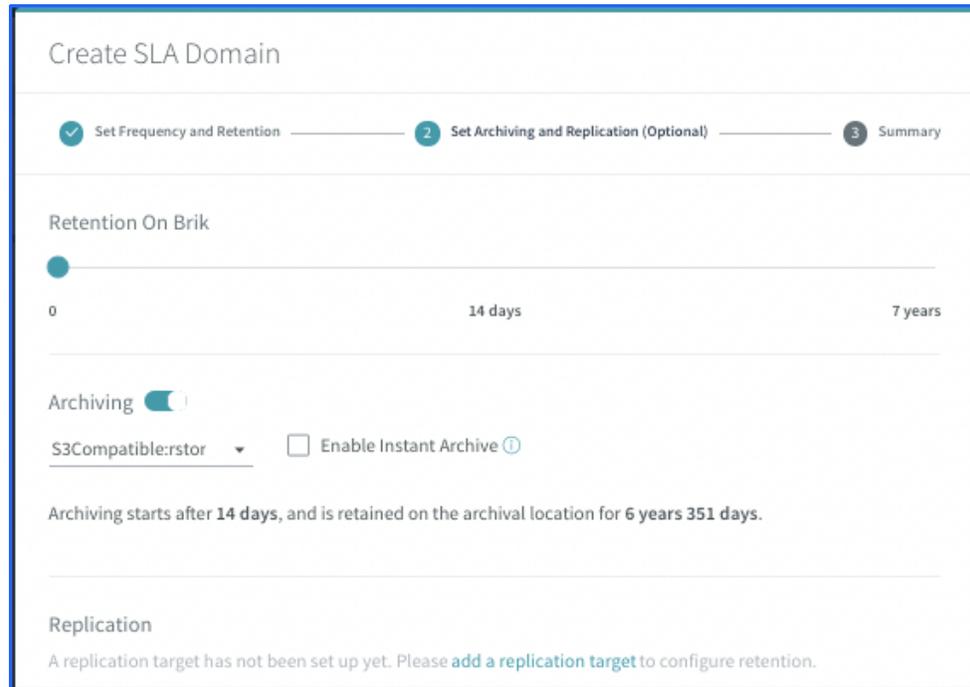
Local retention set to 7 years.

Snapshot Window
Take snapshots from: : to : :
Take first full between: First Opportunity at : :
Cancel Next

14. Click the Archiving toggle and select the RSTOR Archive from the dropdown list. Note that a Rubrik Cluster may have multiple archives attached.

Move the "Retention on Brik" slider bar to determine when the backups will be Archived to RSTOR. Rubrik will expire backups in the Archive based upon the retentions set on the previous page. Click "Next" then "Create". The SLA can now be assigned to objects to be protected by Rubrik, and archiving will automatically happen based upon the SLA's.

In this example backups will be Archived after 14 days.



Create SLA Domain

1 Set Frequency and Retention — 2 Set Archiving and Replication (Optional) — 3 Summary

Retention On Brik

0 14 days 7 years

Archiving

S3Compatible:rstor Enable Instant Archive ⓘ

Archiving starts after 14 days, and is retained on the archival location for 6 years 351 days.

Replication

A replication target has not been set up yet. Please [add a replication target](#) to configure retention.

2.1 Instant Archiving Note

When creating an SLA, there is an option to instantly archive backups. Backups are archived shortly after they've been taken and will reside in the archive for the retention period defined by the SLA before being expired.

Because of this, there may be some snapshots that exist in the RSTOR archive for a short period of time. The snapshots are synthetically created from forward and reverse snapshot chains, so the data expired will be relative to the size of the "deltas" between the backups. This could also potentially lead to ghost data being reported.

Customers typically only select "Instant Archive" if they are not replicating backups between Rubrik Clusters for DR and want to have backups off sited to cloud to provide some ability to recover data in the event of a catastrophic event at their one location.

Create SLA Domain

1 Set Frequency and Retention ————— 2 Set Archiving and Replication (Optional) ————— 3 Summary

Retention On Brik

0 ————— 14 days ————— 7 years

Archiving

S3Compatible:rstor ▾ Enable Instant Archive ⓘ

Instant Archive sends policy-based snapshots to the archival location as soon as they are processed and retains them at the archival location for the maximum retention period specified by the associated policy.

Replication

A replication target has not been set up yet. Please [add a replication target](#) to configure retention.