An Introduction to Rubrik for MongoDB Data Protection

RECENT HISTORY OF BACKUP & RECOVERY SOLUTIONS

MongoDB is a versatile, open-source NoSQL database management system known for handling large volumes of data. It is used across various industries and applications to store, retrieve, and manage data efficiently. MongoDB offers flexibility and scalability for web applications, mobile apps, e-commerce platforms, or big data analytics. It is a popular choice for developers and organizations seeking a robust database solution. As a result, protecting data stored in MongoDB is critical for IT operations to help ensure business continuity, compliance requirements, ransomware threats, and disaster recovery. Typically, organizations have more than one database, such as Oracle, Db2, SAP HANA, and MongoDB, in their environment to meet all their application requirements. The next logical step for their IT team is to enforce data and application protection and have recovery options ready should they become necessary because of natural disasters, infrastructure outages or failures, user errors, or cyber-attacks. A comprehensive data backup and recovery strategy is essential to minimize any downtime and potential data loss.

Oftentimes, native tools lack comprehensive functionality and have limitations. These tools:

- Do not protect against cyber/ransomware attacks
- The requirement of full backup every time leads to inefficiency across compute and storage
- Increased operational complexity because of silos of different databases
- Do not offer a single automated SaaS platform to create and manage data protection across on-premises, public cloud, and hybrid infrastructure
- Either not designed for data protection or not a scalable solution

WHAT IS RUBRIK FOR NATIVE MongoDB DATA PROTECTION?

Rubrik has extended its support portfolio to protect MongoDB by adding native protection via Rubrik Backup Service (RBS). This integration allows enterprises to auto-discover MongoDB workload while consolidating data protection and data lifecycle management under one platform, Rubrik Security Cloud (RSC). RSC is a Software-as-a-Service (SaaS) platform used to centrally manage your MongoDB and other workloads simply through your web browser. RSC offers a single pane of management capabilities for all workloads (on-premises, cloud-native, as well as SaaS) throughout all deployments.

Rubrik provides native automated protection for MongoDB, writes backups directly to Rubrik's immutable file system for resiliency against ransomware attacks, and provides out-of-the-box compliance reports and monitoring. Rubrik has traditionally offered support of MongoDB protection via software-only plane Mosaic that needed separate appliances and hardware. With the latest release, Rubrik's native MongoDB protection offers similar ease of use and out-of-the-box experience to the native protection of VMware, Oracle, SQL, SAP HANA, IBM Db2, and other such workloads.

To protect MongoDB, Rubrik uses an incremental forever approach, i.e., after taking a first full backup, Rubrik leverages MongoDB oplogs and performs post-processing on top of the last backup to create a virtual full backup, as per the SLA frequency. This provides a backup chain that rolls forward in time at each collection level.

Rubrik uses this chain to provide control to users in supporting any point-in-time recovery, from as granular as a single collection to all databases inside MongoDB. The MongoDB user just needs to have permission to insert documents and apply logs in case of performing any point-in-time recovery. Rubrik also offers the flexibility to recover to any other MongoDB cluster irrespective of the topology and thus does NOT restrict just to the MongoDB cluster from the backup was taken and thus an advantage over other rudimentary or physical backup solutions

RUBRIK FOR MongoDB DATA PROTECTION KEY FEATURES

The new solution comes with the following salient capabilities for data protection:

Automated Discovery:

- As MongoDB clusters are added to Rubrik as sources, all the underlying user-defined MongoDB database and collections are automatically discovered during day 0 operations
- Rubrik automates the protection of auto-discovered and new objects post-SLA assignment

Declarative SLA Policy Engine:

- Streamline the protection of MongoDB databases by assigning SLA policies that configure backup frequency, retention, archiving, and replication using the same engine

Native Protection Benefits

- Reduce storage cost via semantic deduplication where Rubrik ensures writing only a golden copy of MongoDB data from its internally replicated data copies across the replicas
- Consistent snapshots across MongoDB nodes ensure a repair-free and, thus faster recovery of data
- Flexibility to recover data to unlike topology target MongoDB cluster ensures seamless movement of data across dev-QA clusters

Point-in-Time Granularity:

- Leverage data and log backups to enable collection-level point-in-time recovery
- Roll forward log backups on top of data backups for granular control over recovery points.

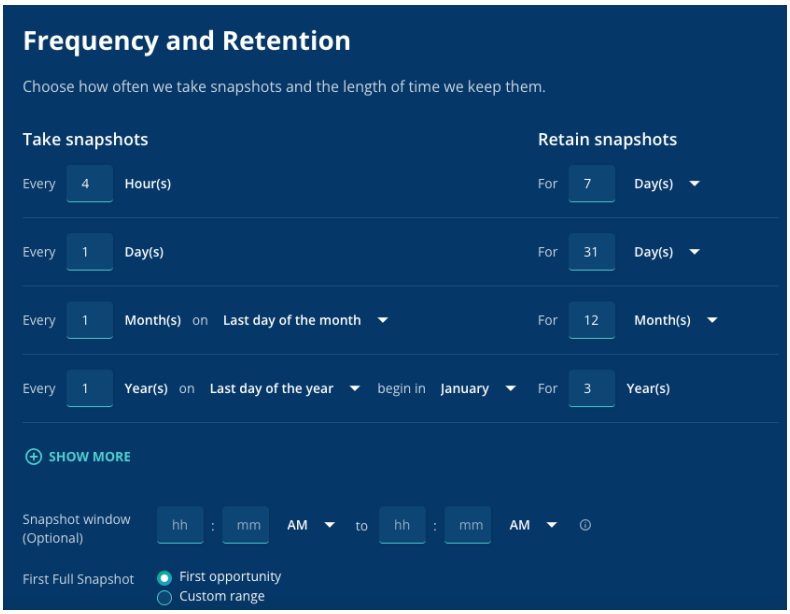
Unified Management and Reporting Platform:

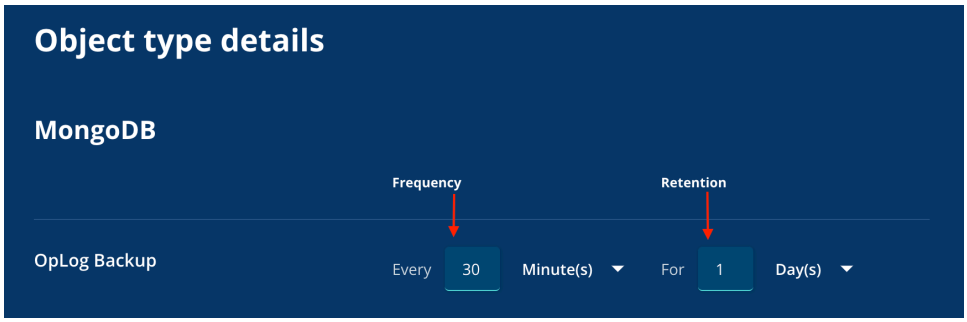
- Keep your MongoDB and other databases, along with other datacenter objects, protected across on-premises and cloud with centralized visibility and control.
- Active Monitoring: View the status of your MongoDB data backup from a centralized activities pane.
- Comprehensive SLA Compliance Reporting: View backup summary information and the latest recovery points, and identify which backups have failed across your environment.

RUBRIK FOR MongoDB ARCHITECTURE OVERVIEW

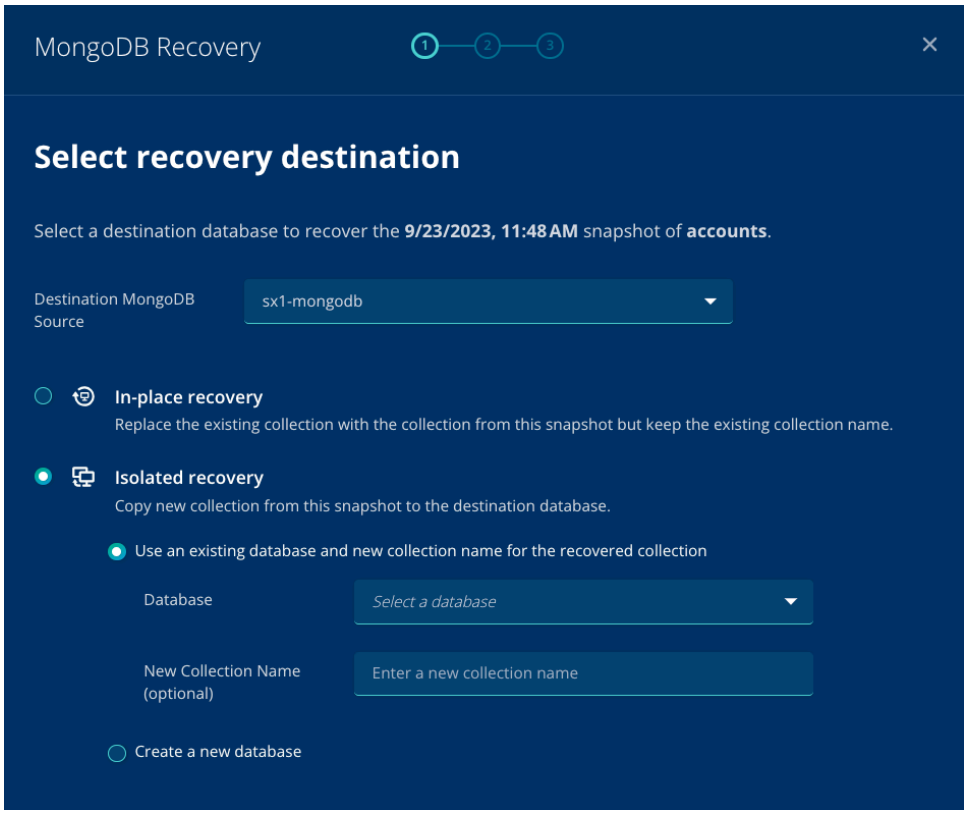
Rubrik provides an innovative, proprietary approach for MongoDB to deliver a powerful data protection solution. The following diagram describes a high-level overview of this protection.

- The Rubrik Backup Service (RBS) software is deployed on the MongoDB host, via deb or rpm installation methods. The download links can be obtained from RSC. Rubrik will automatically detect if any node in the cluster is not associated with an RBS until explicitly added to the exception list of nodes that don't need to be protected.
- The MongoDB sources are added to the RSC by the administrator, and then the RSC automatically discovers underlying databases and collections. Rubrik uses the control plane flow to retrieve the metadata, then uses this metadata to add the MongoDB source and discover the databases.
- Once discovered, customers can assign SLA Policies from RSC, which automates protection frequency and retention for full database or log backups.





- Rubrik uses the data path to ingest MongoDB data to Rubrik's immutable file system and retrieve the backups for recoveries. The data path uses the NFSv3 protocol to write directly to an immutable file system to store MongoDB backups and logs.
- The external and internal communications between protected objects, Rubrik Cluster, your cloud accounts, and the RSC are encrypted. The control path communication between Rubrik Cluster and RSC is always encrypted via TLS 1.2 protocol. All communication from Rubrik Cluster to MongoDB nodes occurs via RBS over Thrift protocol.
- Although MongoDB has a native backup solution for granular recovery and point-in-time recovery, those APIs are not exported to third-parties.. To solve this challenge, Rubrik has developed an innovative approach to back up MongoDB using the native client library interface to collect documents and Oplogs.
- Oplog backup for MongoDB starts before the start of full backup to capture the changes during full backup to create a consistent backup image, while the database is still online.
- There are multiple recovery options supported with Rubrik:
  - » Recover single or multiple databases. This option recovers all collections inside the database(s).
  - » Recover single or multiple collections. This recovers one or multiple collections inside a single database.



- The recovery operation leverages the closest point in time or the latest point in time snapshots. The snapshot chain is directly mounted to the chosen snapshot along with Oplog. RBS then performs the recovery on the host side. Once the recovery operation is complete, RBS unmounts the snapshots. Rubrik also ensures that only one restore job is running for the required objects to be restored.
- Recovery options include in-place or isolated recovery to another target MongoDB source or the same source.

CONCLUSION

Rubrik provides modern data protection for industry-leading databases, offering you comprehensive functionality with the following key benefits:

- Protects you against cyber/ransomware attacks
- Single converged SaaS platform that unifies and automates the protection of your physical and virtualized databases across on-premises and the cloud
- Manage your entire data lifecycle with a single SLA Policy Engine
- Granular and topology-independent recovery options to recover your data
- Designed to scale with your data

To learn more, check out: https://www.rubrik.com/solutions/mongodb

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

brf-an-introduction-to-rubrik-for-mongodb-data-protection-tech-brief / 20231018