TECHNICAL WHITE PAPER

Protecting Microsoft SQL Server with Rubrik

Rubrik Technical Marketing

March 2023
RWP-0615

Table of Contents

ABSTRACT

Microsoft SQL Server has become a crucial component of applications used worldwide. Thanks to its robust database services and widespread adoption, it is often the trusted source for sensitive company data. As a result, protecting data stored in Microsoft SQL Server is critical for IT operations to help ensure compliance with regulations and disaster recovery. Rubrik integrates with Microsoft SQL Server to offer a policy-driven approach to database protection, providing secure management of the backup data lifecycle. Despite the potential complexity of Microsoft SQL Server environments, the Rubrik integration aligns with the core architectural and operational simplicity of Rubrik.

AUDIENCE

The purpose of this white paper is to assist Backup Administrators and Database Administrators (DBAs) in comprehending the advantages and best practices for implementing Rubrik to protect Microsoft SQL Server.

RUBRIK SECURITY CLOUD

Rubrik Security Cloud is a Software-as-a-Service (SaaS) platform that enables you to keep your data secure and quickly recover your data wherever it lives—across the enterprise, in the cloud, and in SaaS applications. Rubrik offers many data protection and security solutions, such as Enterprise Data Protection for your databases, VMs, physical machines, etc., with air-gapped, immutable, access-controlled backups. Visit the Rubrik Security Cloud website for more details.

aws
SAP HANA
vmware
SQL Server

Rubrik Security Cloud™

Data Resilience

Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups.

- Enterprise Data Protection
- Cloud Data Protection
- Microsoft 365 Protection

Data Observability

Continuously monitor and remediate data risks, including ransomware, sensitive data exposure, and indicators of compromise.

- Ransomware Monitoring & Investigation
- Sensitive Data Monitoring & Management
- Threat Monitoring & Hunting
- Data Security Command Center

Data Remediation

Surgically and rapidly recover your apps, files, or users while avoiding malware reinfection.

- Threat Containment
- Mass Recovery
- Orchestrated App Recovery
- Cyber Recovery

Rubrik provides Microsoft SQL Server data protection and data management for on-premises infrastructure, Infrastructure as a Service (IaaS) for Amazon AWS, Microsoft Azure, and Platform as a Service (PaaS) for Amazon RDS, Azure SQL, and Azure Managed Instances. This document focuses on the data protection solution for on-premises infrastructure and IaaS systems. See the How it Works: Cloud Native Protection for Amazon RDS white paper for information on the Rubrik integration for PaaS solutions.

NOTE: For conciseness, we will henceforth use the term “SQL Server” to describe Microsoft SQL Server.

KEY BENEFITS

Before diving deeper into the SQL Server best practices, this section will provide an overview of the benefits of Rubrik Security Cloud.

SIMPLIFIED MANAGEMENT, MONITORING, AND REPORTING

- **Auto-discovery** of all hosts, instances, databases, failover clusters, and availability groups (AG) whenever the Rubrik Backup Service is installed, and lowering operational overhead during configuration.
- **Auto-inheritance** of policies. Simply assign SLA policies to SQL Server, and all instances and databases inherit the policy.
- **Centralized management** via visibility in Rubrik Security Cloud of all databases, protected or otherwise.
- **Real-time reporting** of failures, backups, object protection status, compliance, infrastructure capacity, etc., across on-prem and cloud environments

OPTIMIZED DATABASE PROTECTION

- **Incremental-forever** backups reduce local storage requirements and improve backup times.
- **Full application awareness** in high availability deployments like Always On Availability Groups and Windows Failover Clustered Instances.
- **Granular database protection** via Rubrik SLA policies—the ability to have different policies at the server, instance, and database level.
- **Change block tracking (CBT)** substantially reduces the backup times of large databases.
- **Log backup, log shipping and log management**, further reducing operational time.
- **Copy-only mode** for seamless transition or coexistence with existing backup products.

EXPEDITED RECOVERY

- **Seamless point-in-time restore** enabled in a single operation.
- **Live Mount** delivers near-zero RTOs by mounting SQL databases directly on Rubrik.
- **Automation** provides key integrations and automated recoveries.

These capabilities and more will be explored in the upcoming sections.

SETUP

Rubrik supports the same versions of SQL Server as Microsoft via extended support. Please see the Rubrik Compatibility Matrix (available in the Customer Support Portal) for supported version details.

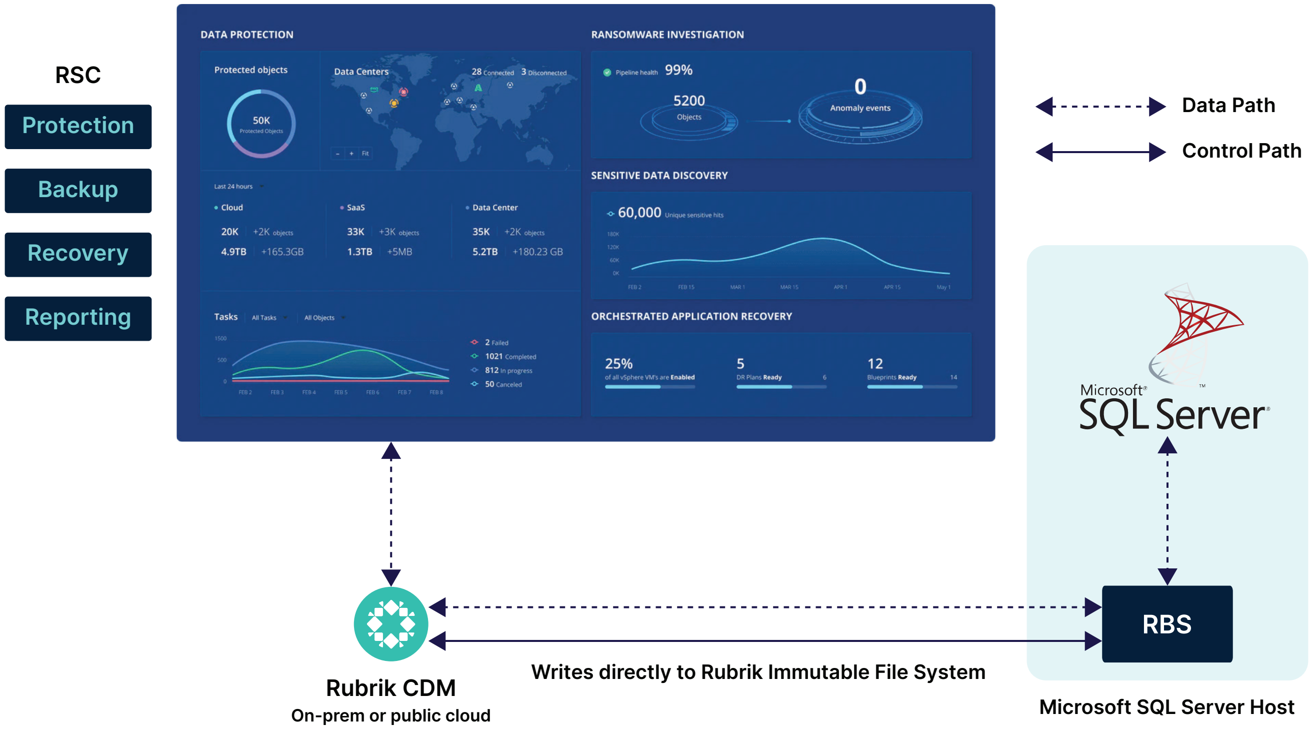
RUBRIK BACKUP SERVICE (RBS)

The Rubrik Backup Service (RBS) is a lightweight SQL Connector that provides enhanced integration with SQL Server protected resources and host systems. Installing RBS on a SQL Server allows for the backup and restoration of SQL databases. It can be downloaded and installed when adding a Windows Server host. It then runs as a Windows service named RBS. RBS may be installed anytime, as no reboot is required. This allows you to choose when to transfer data protection to Rubrik without disruption to service.

Connector upgrades are automatic and completely transparent to the user after installation to reduce operational overhead. Once RBS is installed, SQL instances and databases are automatically discovered. You can assign an SLA domain at the host, instance, AG, or database level—these policies are core to Rubrik and can be leveraged across multiple data types.

After the RBS is installed, it uses the local system account permissions. This account level permissions should be changed to an Active Directory based service account which is a member of the local administrator group on the server. This enables Rubrik to perform recovery operations. The account level can be set to sysadmin also, but it is not required.

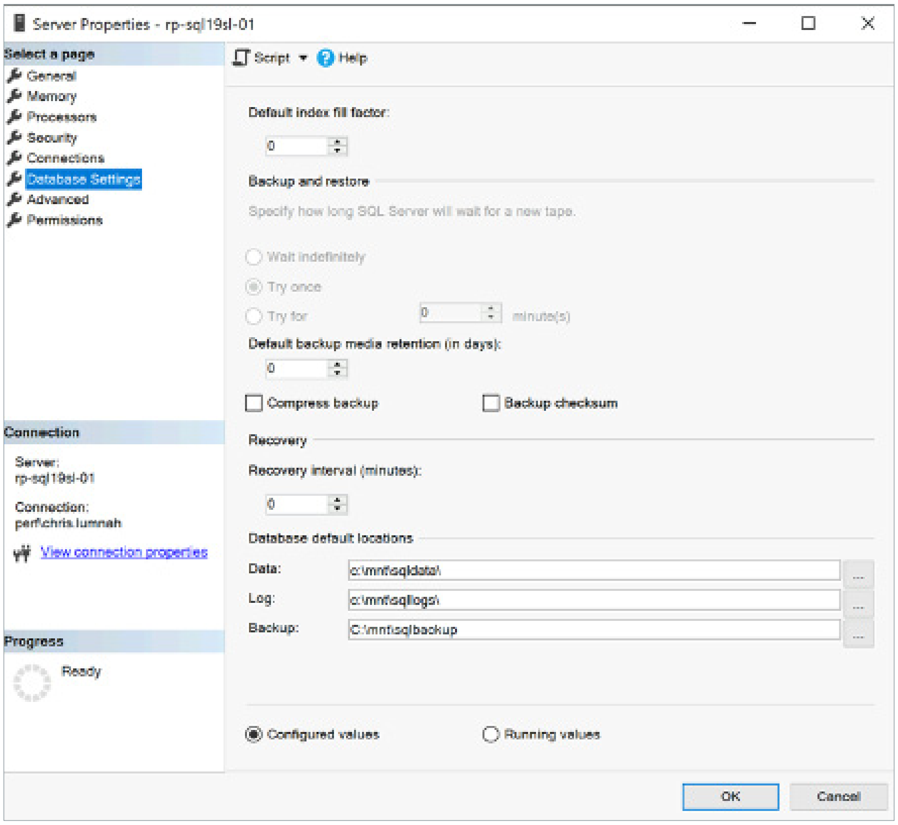
The connection between RBS and Rubrik is established through secure channels, with the RBS installer containing a unique CDM certificate.



After installation, RBS generates a new public/private key for the host. The host is subsequently added to Rubrik CDM through RSC. Rubrik CDM isn't aware of the host's identity, it operates under the Trust On First Use (TOFU) principle. Upon adding the host, CDM acknowledges and trusts the host's identity. In most cases, the communication with RBS is initiated by Rubrik CDM over the control path. The backup data transfer takes place over the data path using the Secure Thrift protocol to ensure end-to-end secure communication.

Default Log Backup Location

If the RBS doesn't have sysadmin access when Rubrik takes a log backup of a SQL Server database, it will write to a temporary location on the C drive. This temporary location is used for both the log backup and restore. Once the operation is done, the files are removed from the temporary location. Rubrik allows the DBAs to control where this temporary location resides. The DBA can control this by going into SQL Server Management Studio (SSMS) and updating the default backup location.



Server Properties - rp-sql19sl-01

Default index fill factor: 0

Backup and restore

Specify how long SQL Server will wait for a new tape.

○ Wait indefinitely
● Try once
○ Try for 0 minute(s)

Default backup media retention (in days): 0

□ Compress backup □ Backup checksum

Recovery

Recovery interval (minutes): 0

Database default locations

Data: c:\mnt\sqldata\
Log: c:\mnt\sqllogs\
Backup: C:\mnt\sqlbackup

● Configured values ○ Running values

Connection

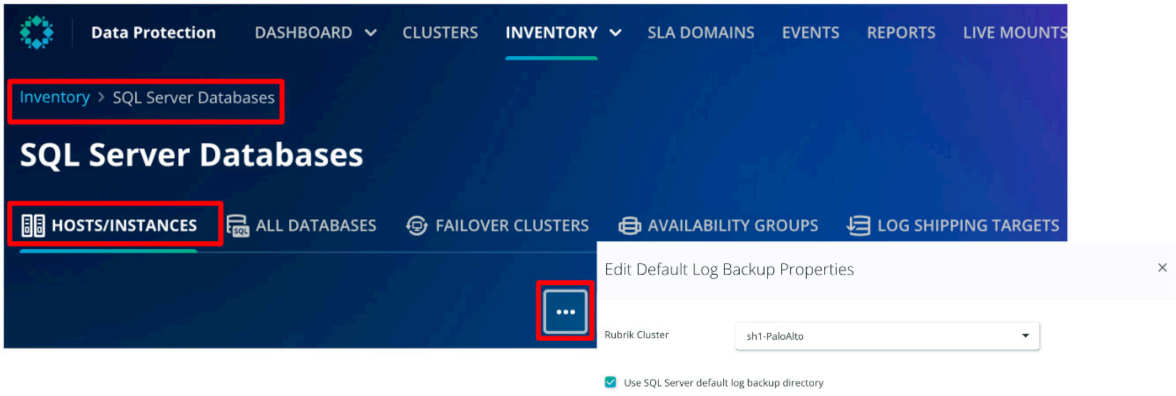
Server:
rp-sql19sl-01

Connection:
perf\chris.lumnah

Progress

Ready

Rubrik can be configured to use the location specified by the DBA for log backups or the default location via the RSC.



Inventory > SQL Server Databases

SQL Server Databases

Edit Default Log Backup Properties

Rubrik Cluster: sh1-PaloAlto

☑ Use SQL Server default log backup directory

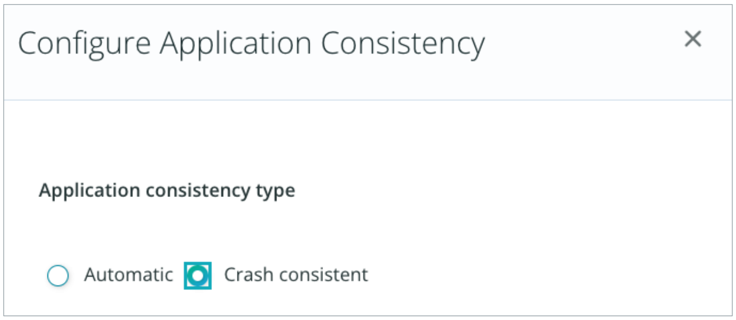
VM CONFIGURATION

When Rubrik is configured to protect a virtual machine, it automatically starts taking application consistent backups, which provide a point-in-time snapshot with quiescence and application awareness. To achieve the highest level of backup consistency, the Rubrik cluster requires RBS installation and registration, along with an up-to-date version of VMware Tools.

During the process of taking application consistent snapshots, everything on the virtual machine, including database files, is temporarily frozen or quiesced. This ensures that all IO operations are paused while the snapshot is being created, which usually takes only a few seconds. During this time, applications and users are not affected, but the databases may experience timeouts and service interruptions. Additionally, the SQL Server VSS Writer is activated, which registers a Copy Only Full Backup in msdb. However, this can be misleading to the DBA since no actual database backup is generated. To avoid this, Rubrik recommends the following two options:

Set crash-consistent backup

The first option is to switch the VM's application-consistent snapshots to crash-consistent snapshots, which can be done through RSC.


Configure Application Consistency

Application consistency type

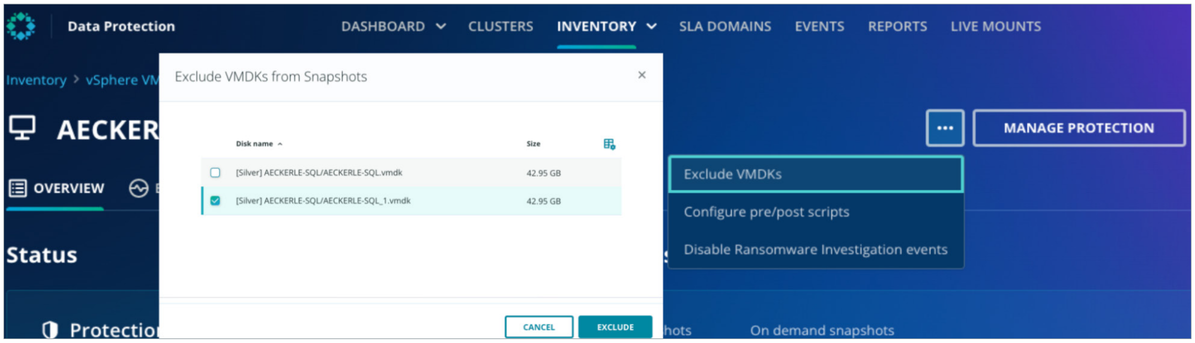
○ Automatic ● Crash consistent

By implementing application crash consistency, the SQL Server VSS Writer is not utilized, and no additional backup is written to msdb, eliminating any confusion. Moreover, databases and files are not quiesced, and IO operations are not paused, thus not causing any service interruption to the queries and users.

Assigning an SQL database SLA policy can help maintain database availability by ensuring timely database snapshots and log backups. In the event of a disaster, you can recover the entire virtual machine with its disks and then restore the databases to the desired point in time.

Exclude VMDKs

The second alternative is to exclude the VMDKs that contain your SQL database files from the VM snapshot, which can be configured for the VM using RSC.



Exclude VMDKs from Snapshots

	Disk name	Size
□	[Silver] AECKERLE-SQL/AECKERLE-SQL.vmdk	42.95 GB
☑	[Silver] AECKERLE-SQL/AECKERLE-SQL_1.vmdk	42.95 GB

When you exclude the VMDKs, the VM will receive an application snapshot that does not include the disks containing the database file. This means that the database files will not be included in the snapshot, and the VM snapshots will not quiesce the database files, thus allowing IO operations to continue.

Additionally, the VM snapshots will not create any copy-only backup records in the msdb. In case of a disaster, you can restore the entire VM without the disks hosting the database file. Subsequently, you will need to attach new VMDKs before commencing the process of restoring the databases.

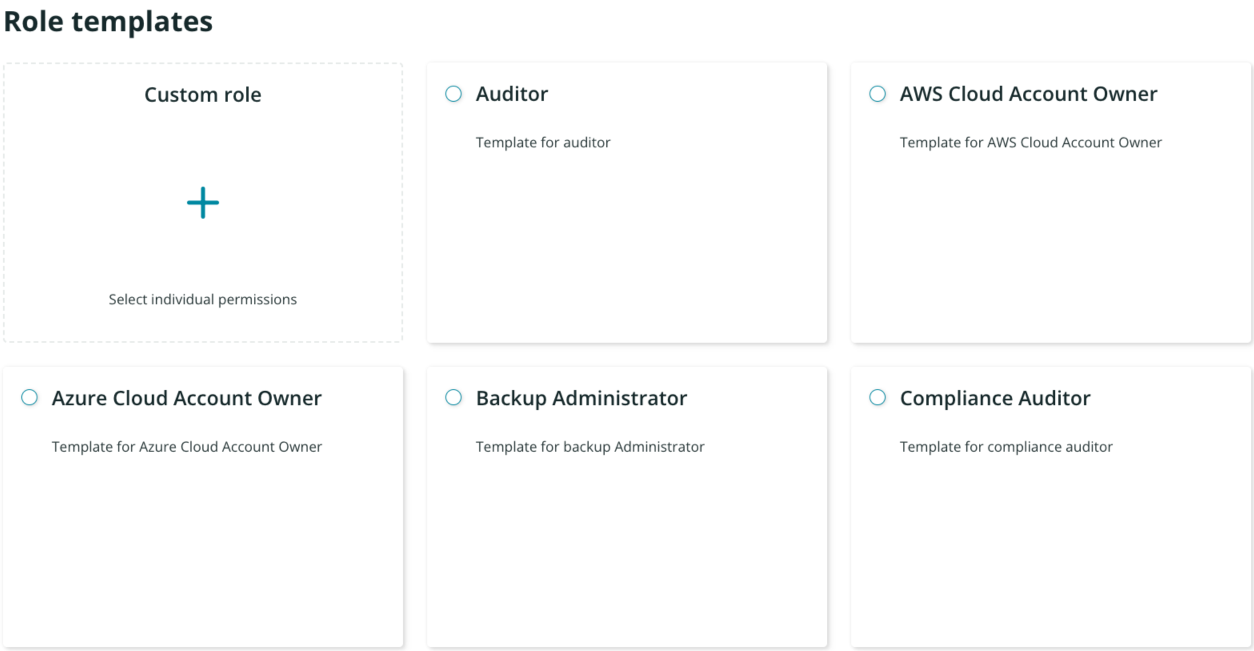
ROLE-BASED ACCESS CONTROL (RBAC)

RSC provides role-based access control, and several methods for authenticating a user account.

RSC offers role-based access control (RBAC) that regulates access based on the roles of individuals within an organization. Depending on the assigned role, access rights are restricted to the relevant associated information and resources. Permissions are assigned to specific roles, and roles are assigned to user accounts.

RSC provides RBAC that enables administrators to restrict access to authorized users and to facilitate the administration of users and permissions.

RSC user management also helps to preserve organizational hierarchy and maintain the least privilege security model by limiting the accessible account functions. RBAC restricts access to features and resources within a Rubrik cluster to authorized users or groups. Visit the RSC user guide to read about the user and role permissions.



Role templates

Custom role

+

Select individual permissions

○ Auditor

Template for auditor

○ AWS Cloud Account Owner

Template for AWS Cloud Account Owner

○ Azure Cloud Account Owner

Template for Azure Cloud Account Owner

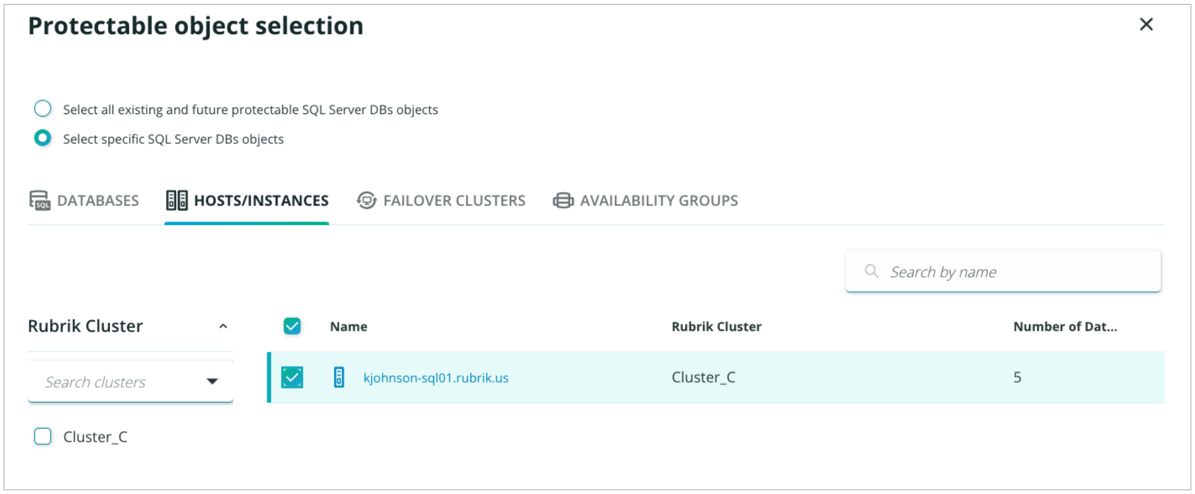
○ Backup Administrator

Template for backup Administrator

○ Compliance Auditor

Template for compliance auditor

For example, let's say that we want to create a role for the help desk that has permission to recover any database, but only through a Live Mount or Export operation, both of which are non-destructive restore operations. We first use the slider to *select all current and future protectable objects* and then define the individual permissions by selecting *Live Mount and Export* operations.



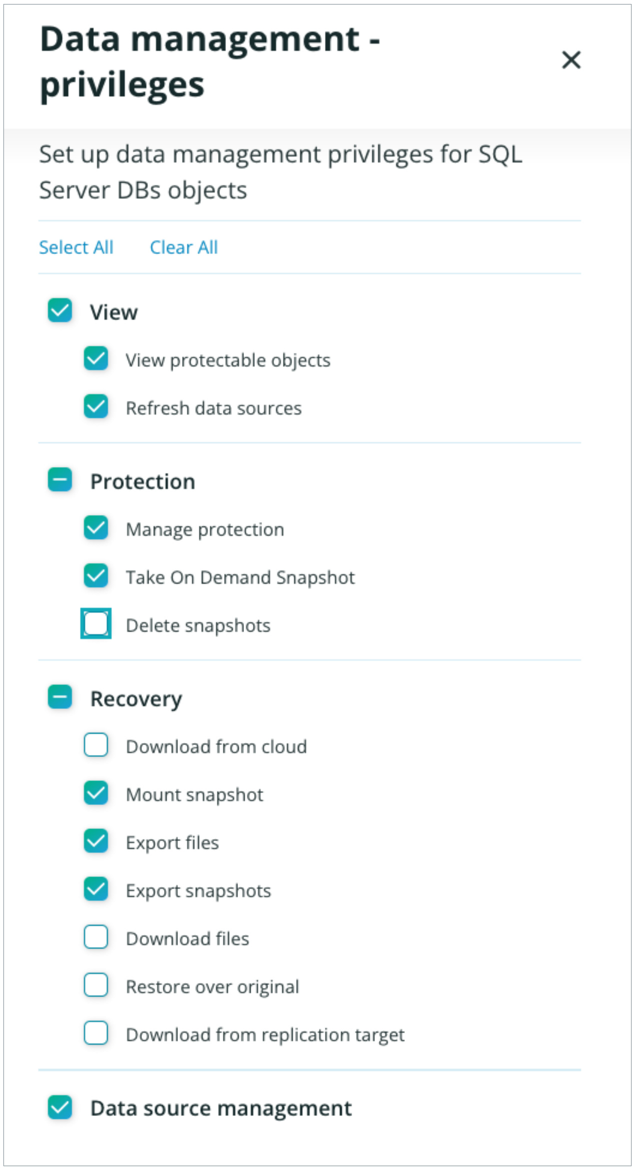
Protectable object selection

○ Select all existing and future protectable SQL Server DBs objects

● Select specific SQL Server DBs objects

□ Cluster_C

☑	Name	Rubrik Cluster	Number of Dat...
☑	kjohnson-sql01.rubrik.us	Cluster_C	5



Data management - privileges

Set up data management privileges for SQL Server DBs objects

☑ View
- ☑ View protectable objects
- ☑ Refresh data sources

⊟ Protection
- ☑ Manage protection
- ☑ Take On Demand Snapshot
- □ Delete snapshots

⊟ Recovery
- □ Download from cloud
- ☑ Mount snapshot
- ☑ Export files
- ☑ Export snapshots
- □ Download files
- □ Restore over original
- □ Download from replication target

☑ Data source management

If there are any security policy changes or permissions delegation, the role can be modified at any time. This provides you with a flexible and dynamic method of securing their environment and database backups.

DATA PROTECTION

Once the RBS installation is complete, Rubrik automatically discovers all the SQL Server hosts/instances, databases, failover clusters, and AGs. The next step would be to start protecting the SQL Server using Rubrik Global SLA Domain Policy to ensure the reliability and availability of data backups. The goal is to ensure that your organization's data can be quickly and easily restored during a cyberattack or natural disaster.

SLA DOMAIN POLICY

A Rubrik SLA Domain Policy is a declarative policy that captures the core objectives for backup and recovery. It translates the Recovery Point Objective (RPO) requirements for data protection and manages the data from the cradle to the grave. More importantly, it eliminates the need to manually configure jobs, tasks, and other activities to maintain a data protection scheme.

SLA Domains are a core part of the Rubrik architecture. You can add any workload type Rubrik supports to an SLA Domain. This provides you with a simple mechanism to control data protection for different workloads across your on-prem, edge or cloud environments.

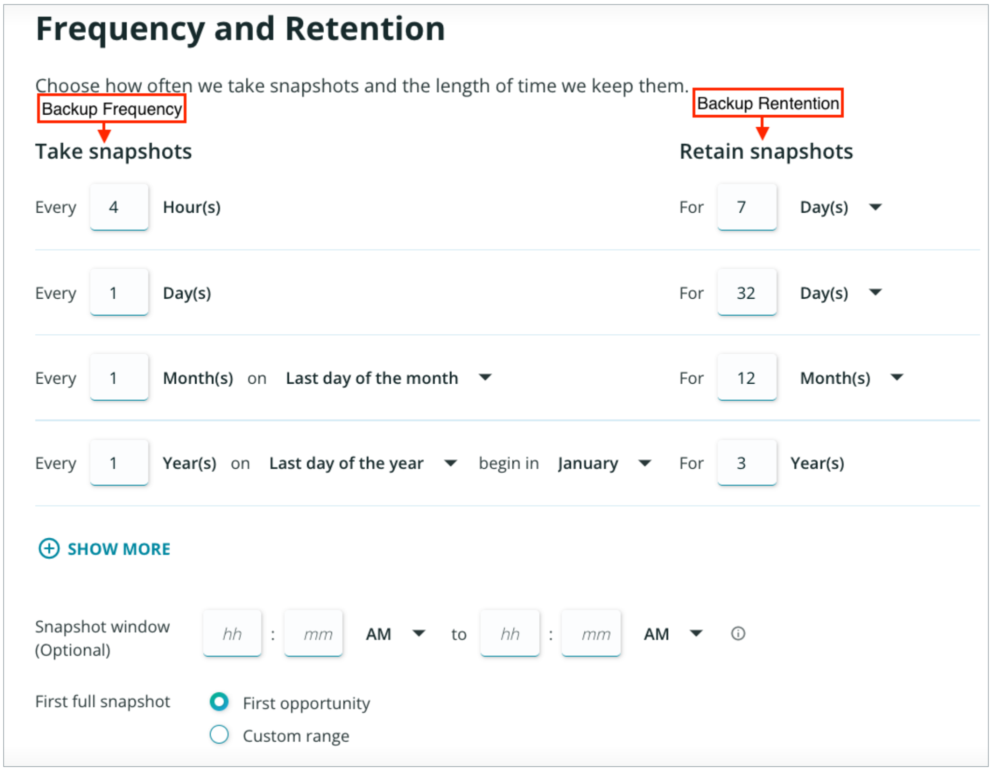
By default, Rubrik preconfigures three SLA Domains providing various levels of hourly, daily, monthly, and yearly snapshot frequency and retention:

- Gold
- Silver
- Bronze

Regular Use SLA Domains

Depending on the RPO and SLA requirements, you might need to configure a custom SLA Domain Policy. Let's walk through the pieces needed to configure an SLA Domain Policy for any object (SQL-specific items will be covered in the next section):

- **Backup Frequency:** also known as the Recovery Point Objective (RPO). Simply put, how often are backups taken?
  - For databases, this determines how often a database restore point is taken. Each restore point is synthesized from incremental blocks in each backup to maintain an incremental forever scheme. If a database is in the Full Recovery model, the RPO is further reduced by transaction log backups.
- **Backup Retention:** indicates the length of time backups are held for a particular backup frequency.
  - You can optionally select the beginning time for the snapshot window. The first full backup is initiated within the specified window. By default, the first full backup occurs when the SQL server or the database has been added.



Frequency and Retention

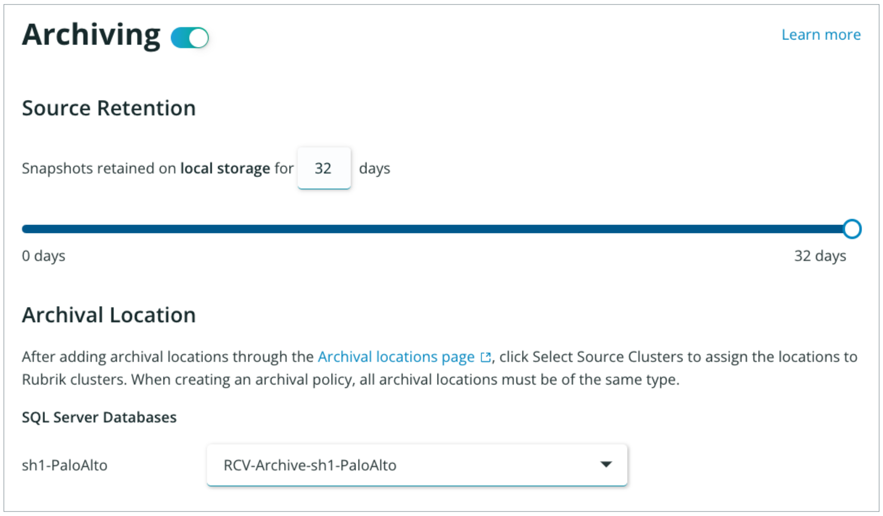
Choose how often we take snapshots and the length of time we keep them.

Take snapshots	Retain snapshots
Every 4 Hour(s)	For 7 Day(s)
Every 1 Day(s)	For 32 Day(s)
Every 1 Month(s) on Last day of the month	For 12 Month(s)
Every 1 Year(s) on Last day of the year begin in January	For 3 Year(s)

Snapshot window (Optional) hh : mm AM to hh : mm AM

First full snapshot ● First opportunity ○ Custom range

- **Archival Policy:** this defines the life cycle of backups during the archival process. It defines when backups are sent to the archive, where they are stored, and the retention of data archived. Archives create an offsite copy of your data in cheaper storage tiers, offering significantly reduced costs. Archive targets can be public cloud (AWS, Azure, GCP, or Rubrik Cloud Vault) or on-premises (S3 compatible object stores, NFS, or tape).
  - For databases, long-term archiving is often stored in a cloud archive such as Rubrik Cloud Vault for regulatory or compliance reasons.
  - Rubrik Cloud Vault offers account-isolated, offsite, immutable copies of your data with authenticated, fully encrypted Azure Blob integration. You can set up your secure, isolated cloud environment directly from RSC in minutes. Visit the Rubrik Cloud Vault webpage to read about the archive solution.



Archiving

Source Retention

Snapshots retained on **local storage** for 32 days

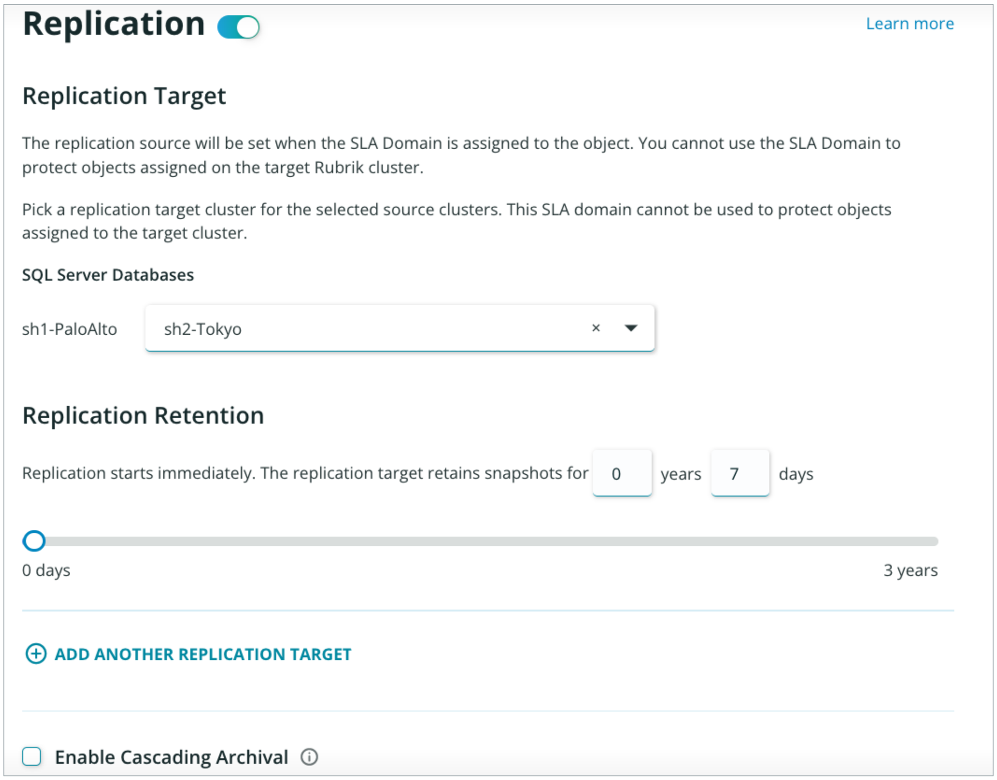
Archival Location

After adding archival locations through the Archival locations page, click Select Source Clusters to assign the locations to Rubrik clusters. When creating an archival policy, all archival locations must be of the same type.

SQL Server Databases

sh1-PaloAlto RCV-Archive-sh1-PaloAlto

- **Replication Policy:** this relates to disaster recovery (DR). Effectively, how long should backups replicated to another Rubrik cluster be kept at a DR site?
  - For databases, this often is a shorter time frame. In a DR situation, recovery of the most recent state of a database is most common.



Replication

Learn more

Replication Target

The replication source will be set when the SLA Domain is assigned to the object. You cannot use the SLA Domain to protect objects assigned on the target Rubrik cluster.

Pick a replication target cluster for the selected source clusters. This SLA domain cannot be used to protect objects assigned to the target cluster.

SQL Server Databases

sh1-PaloAlto: sh2-Tokyo ×

Replication Retention

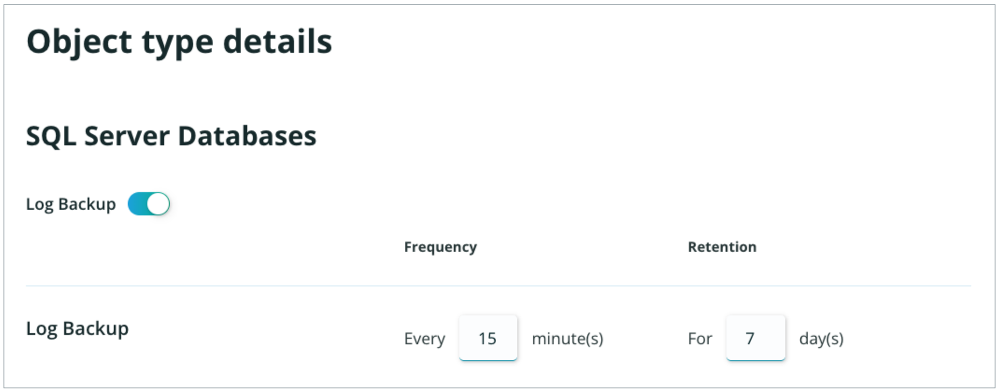
Replication starts immediately. The replication target retains snapshots for 0 years 7 days

0 days — 3 years

ADD ANOTHER REPLICATION TARGET

□ Enable Cascading Archival

- **Log Backup:** This relates to the point-in-time or granular recovery of the SQL Server. You can enable transaction log backup as part of the SLA Policy.
  - The combination of a snapshot of the database and the transaction log backups from the database permits Rubrik to recover a database to the state it was in at a selected point in time.
  - Rubrik automatically replays the transaction logs to ensure granular recovery.



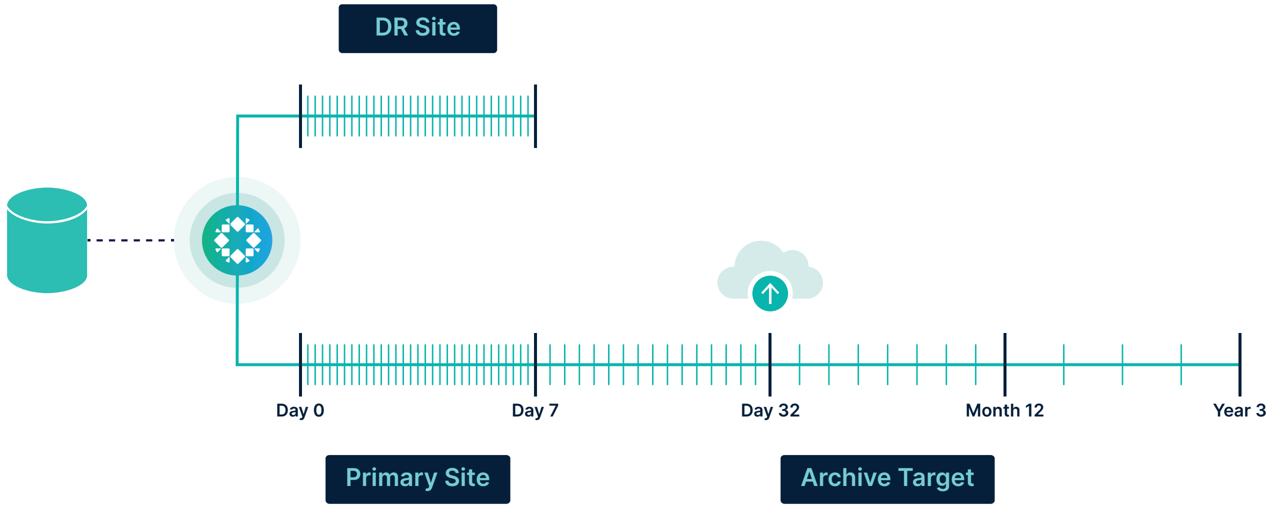
Object type details

SQL Server Databases

Log Backup ●

	Frequency	Retention
Log Backup	Every 15 minute(s)	For 7 day(s)

A visual example of the above SLA Domain policy applied to an SQL Server would look something like this:



As illustrated by the screenshots above, the policy architecture is straightforward to configure yet powerful. Please see the Rubrik User Guide for a more thorough walkthrough of SLA Domain details.

Special Use Case SLAs

As a Database Administrator (DBA), you may encounter various one-time events where you need to take on-demand snapshots before proceeding. These events can include but are not limited to:

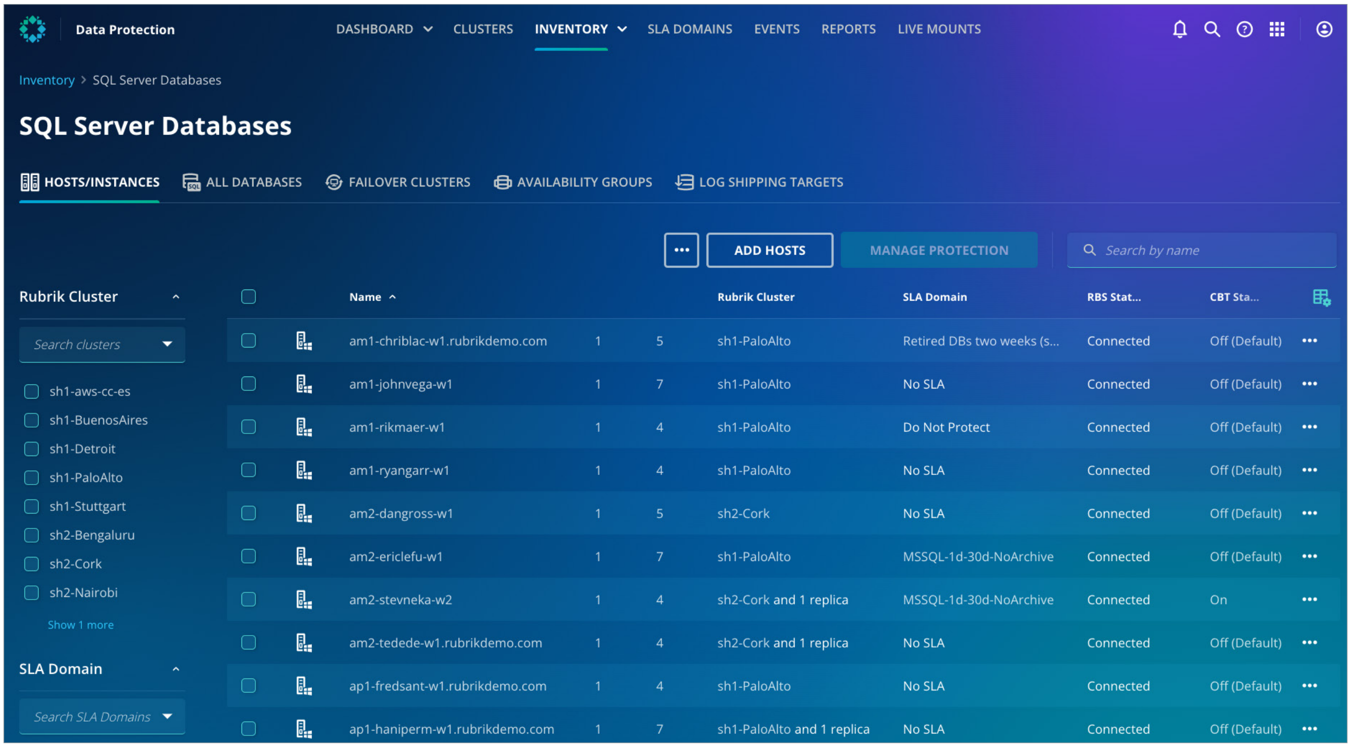
- Code Deployments
- Database Changes
- Patching
- Database or Instance Decommission

Typically, databases or hosts with regular or customized SLAs have longer retention periods for their snapshots. However, for specific events, on-demand snapshots taken just before the event are considered special. This raises the question of whether it's necessary to retain the on-demand snapshot for the entire SLA period, such as 7 years. In such cases, utilizing a Special Use SLA Domain is an appropriate solution. This domain enables the on-demand snapshot to be retained for a shorter period, such as 7 days, instead of the regular SLA period of 7 years. Rubrik automatically expires and deletes the on-demand snapshot after 7 days, resulting in significant savings in storage costs.

SLA DOMAIN ASSIGNMENT

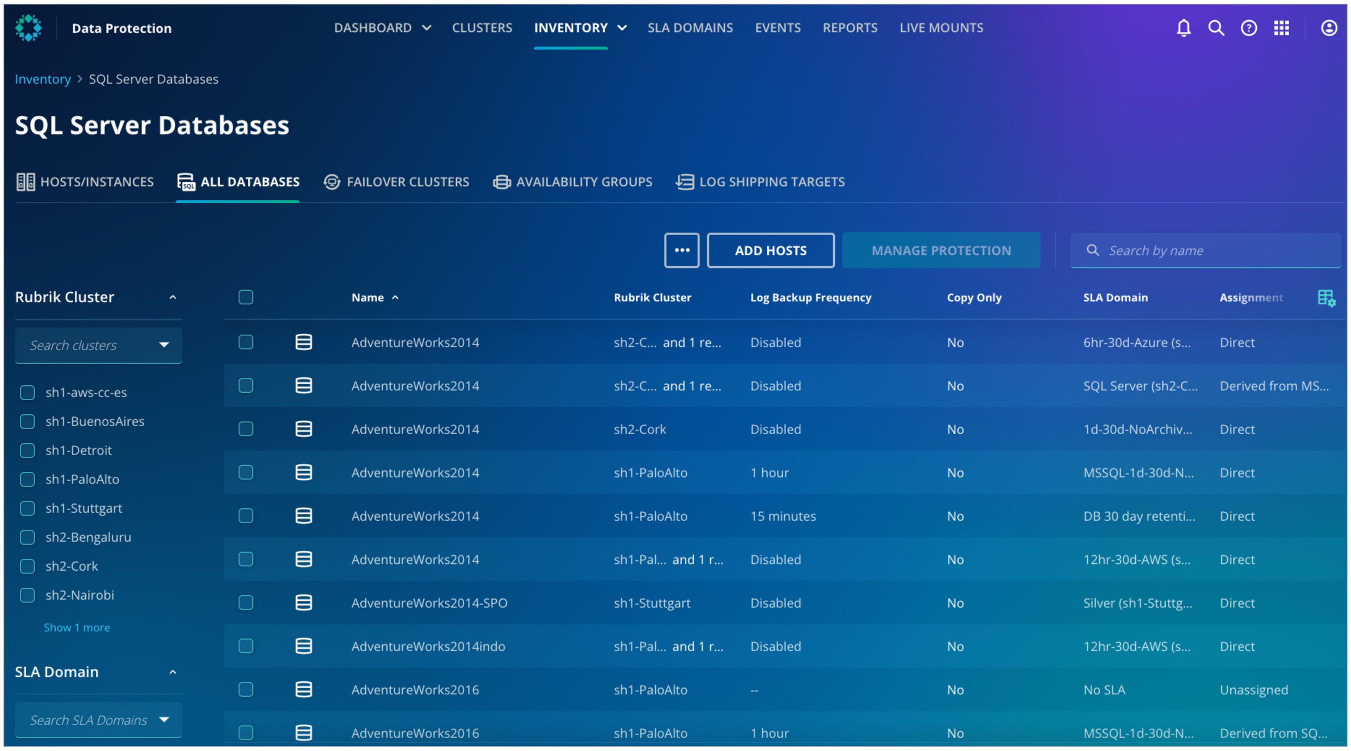
As noted above, SLA Domain Policies can be applied at the SQL cluster, host, instance, AGs, or database level. The following visual walkthrough illustrates this concept and showcases how to configure SQL-specific options.

From the *Inventory* menu, select *SQL Server Databases*. A list of auto-discovered SQL Servers at the host level will be displayed:



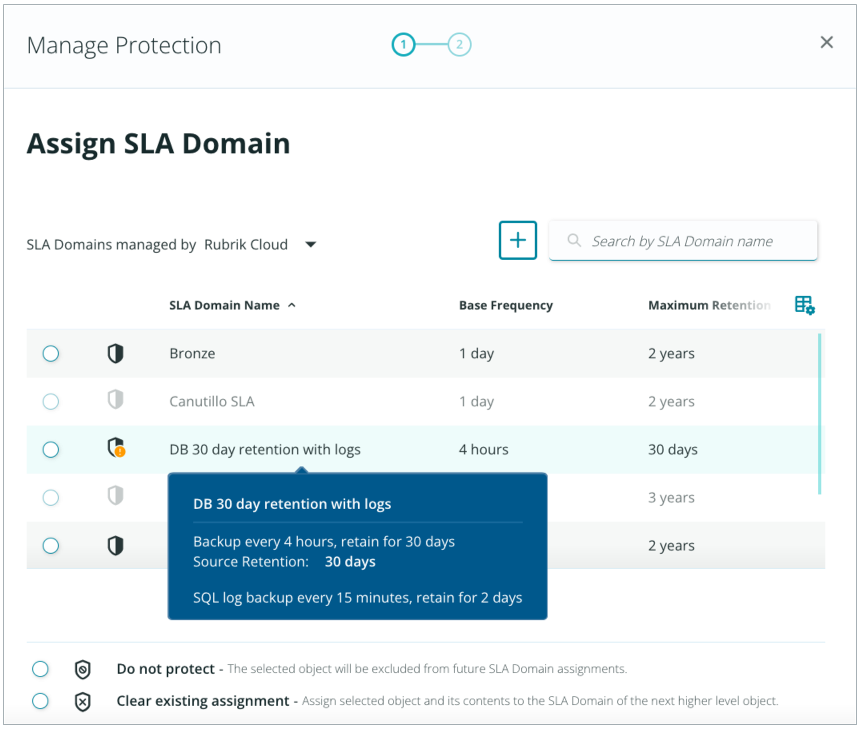
Name			Rubrik Cluster	SLA Domain	RBS Stat...	CBT Sta...
am1-chriblac-w1.rubrikdemo.com	1	5	sh1-PaloAlto	Retired DBs two weeks (s...	Connected	Off (Default)
am1-johnvega-w1	1	7	sh1-PaloAlto	No SLA	Connected	Off (Default)
am1-rikmaer-w1	1	4	sh1-PaloAlto	Do Not Protect	Connected	Off (Default)
am1-ryangarr-w1	1	4	sh1-PaloAlto	No SLA	Connected	Off (Default)
am2-dangross-w1	1	5	sh2-Cork	No SLA	Connected	Off (Default)
am2-ericlefu-w1	1	7	sh1-PaloAlto	MSSQL-1d-30d-NoArchive	Connected	Off (Default)
am2-stevneka-w2	1	4	sh2-Cork and 1 replica	MSSQL-1d-30d-NoArchive	Connected	On
am2-tedede-w1.rubrikdemo.com	1	4	sh2-Cork and 1 replica	No SLA	Connected	Off (Default)
ap1-fredsant-w1.rubrikdemo.com	1	4	sh1-PaloAlto	No SLA	Connected	Off (Default)
ap1-haniperm-w1.rubrikdemo.com	1	7	sh1-PaloAlto and 1 replica	No SLA	Connected	Off (Default)

Database level details:



Name	Rubrik Cluster	Log Backup Frequency	Copy Only	SLA Domain	Assignment
AdventureWorks2014	sh2-C... and 1 re...	Disabled	No	6hr-30d-Azure (s...	Direct
AdventureWorks2014	sh2-C... and 1 re...	Disabled	No	SQL Server (sh2-C...	Derived from MS...
AdventureWorks2014	sh2-Cork	Disabled	No	1d-30d-NoArchiv...	Direct
AdventureWorks2014	sh1-PaloAlto	1 hour	No	MSSQL-1d-30d-N...	Direct
AdventureWorks2014	sh1-PaloAlto	15 minutes	No	DB 30 day retenti...	Direct
AdventureWorks2014	sh1-Pal... and 1 r...	Disabled	No	12hr-30d-AWS (s...	Direct
AdventureWorks2014-SPO	sh1-Stuttgart	Disabled	No	Silver (sh1-Stuttg...	Direct
AdventureWorks2014indo	sh1-Pal... and 1 r...	Disabled	No	12hr-30d-AWS (s...	Direct
AdventureWorks2016	sh1-PaloAlto	--	No	No SLA	Unassigned
AdventureWorks2016	sh1-PaloAlto	1 hour	No	MSSQL-1d-30d-N...	Derived from SQ...

After selecting a host, instance, or database, clicking the *Manage Protection* button brings up the policy assignment screen where users can assign a policy, as well as set options around copy-only backups, log backup frequency, and log backup retention.



Assign SLA Domain

SLA Domains managed by Rubrik Cloud

	SLA Domain Name ^	Base Frequency	Maximum Retention
○	Bronze	1 day	2 years
○	Canutillo SLA	1 day	2 years
○	DB 30 day retention with logs	4 hours	30 days
○			3 years
○			2 years

DB 30 day retention with logs

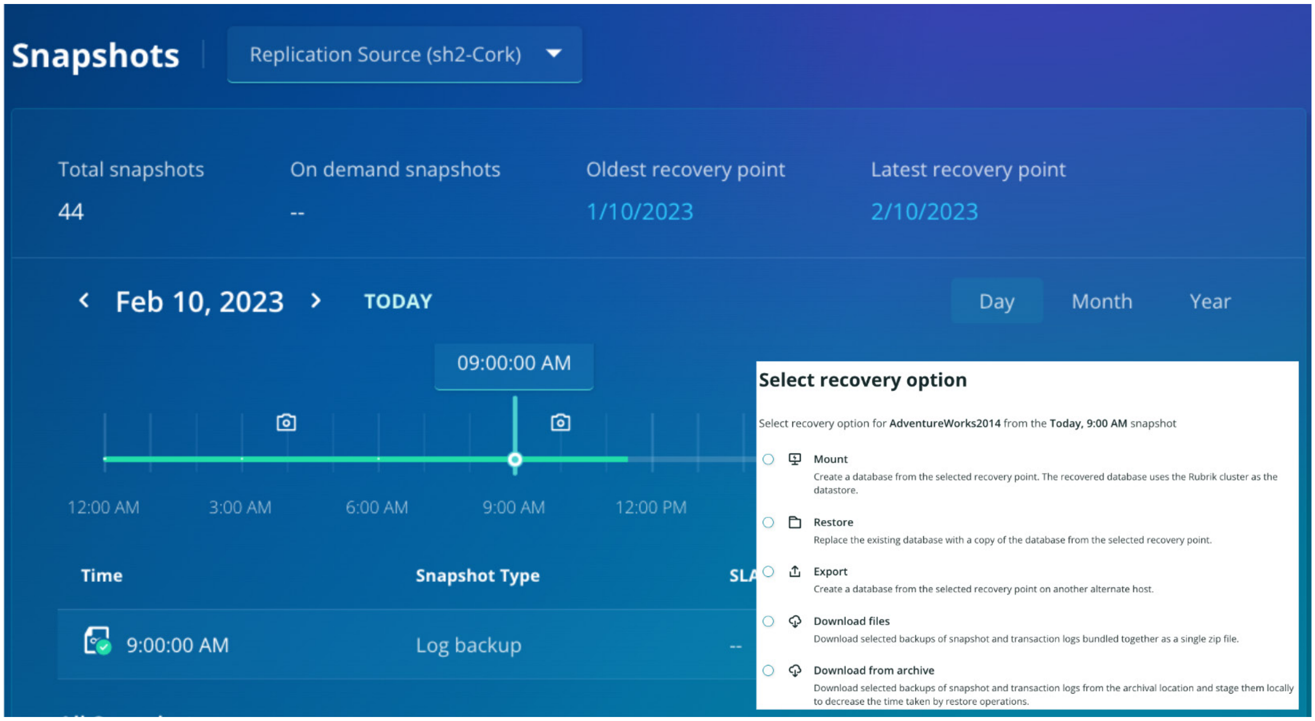
Backup every 4 hours, retain for 30 days
Source Retention: **30 days**

SQL log backup every 15 minutes, retain for 2 days

○ **Do not protect** - The selected object will be excluded from future SLA Domain assignments.

○ **Clear existing assignment** - Assign selected object and its contents to the SLA Domain of the next higher level object.

Once protected, the restore process is a simple slider for point-in-time restore options:



Total snapshots	On demand snapshots	Oldest recovery point	Latest recovery point
44	--	1/10/2023	2/10/2023

Time	Snapshot Type	SLA
9:00:00 AM	Log backup	--

Select recovery option

Select recovery option for **AdventureWorks2014** from the **Today, 9:00 AM** snapshot

○ **Mount**
Create a database from the selected recovery point. The recovered database uses the Rubrik cluster as the datastore.

○ **Restore**
Replace the existing database with a copy of the database from the selected recovery point.

○ **Export**
Create a database from the selected recovery point on another alternate host.

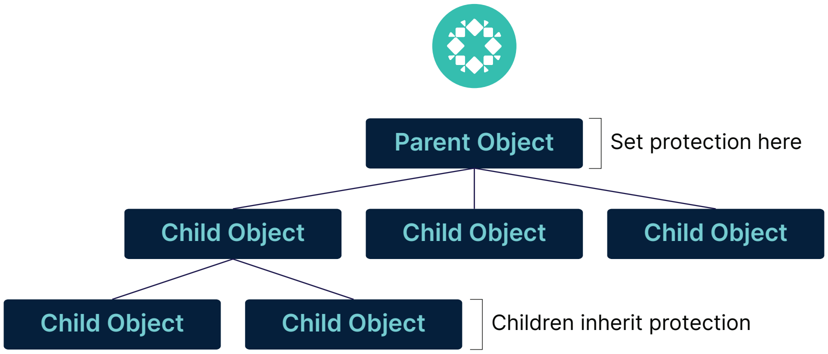
○ **Download files**
Download selected backups of snapshot and transaction logs bundled together as a single zip file.

○ **Download from archive**
Download selected backups of snapshot and transaction logs from the archival location and stage them locally to decrease the time taken by restore operations.

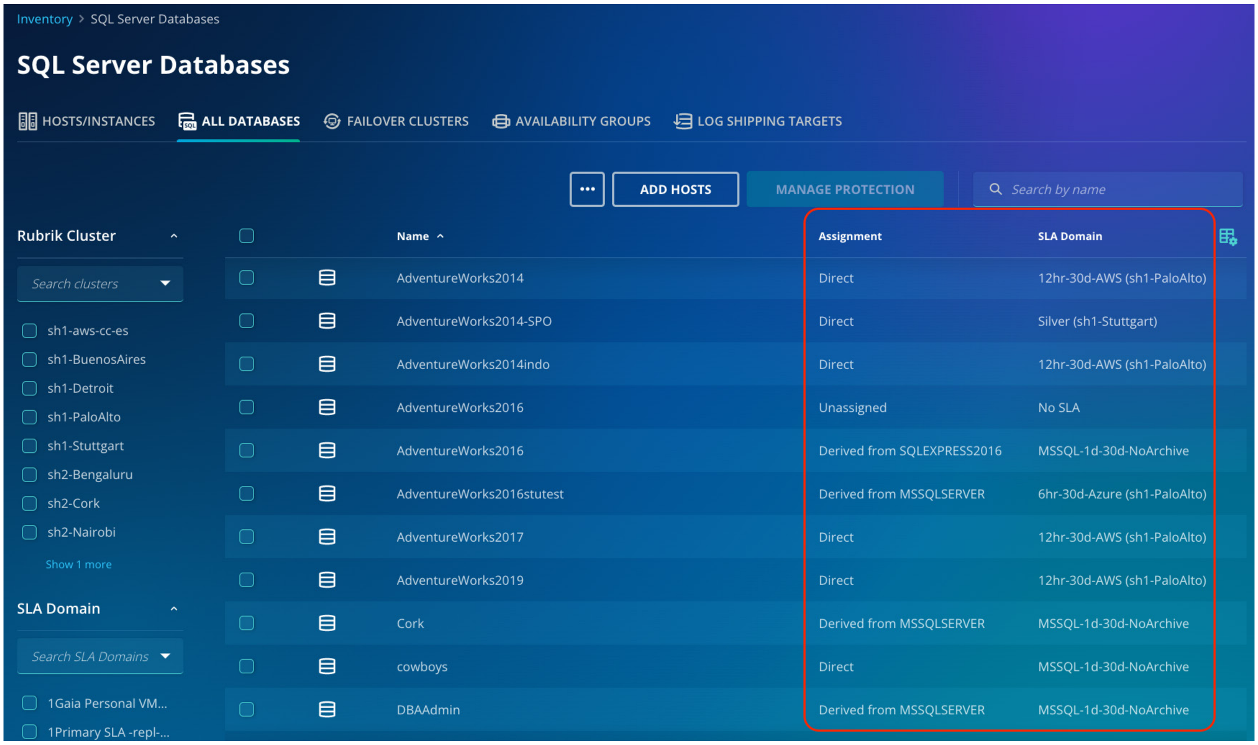
For details about AG configuring, visit the SQL Server AG Configuration page.

GRANULAR DATABASE PROTECTION

SLA domain policies can be assigned at the SQL cluster, host, instance, or individual database level. It is always recommended to assign an SLA Domain at the highest level: in this case, at the host level. By applying an SLA Domain at the highest level, all lower levels will automatically receive the same protection, meaning Host->Instance→Database. For stand-alone hosts, assigning an SLA Domain to the host will ensure that all instances inherit the same policy. Similarly, databases will inherit the policy from their respective instance. Rubrik automatically detects and secures newly added databases to an instance.



In cases, where you have a host with multiple instances, you can assign a different policy for each instance to meet your business requirements. For more stringent RPO and RTO requirements, granular SLAs can be configured and assigned at database levels.



Name	Assignment	SLA Domain
AdventureWorks2014	Direct	12hr-30d-AWS (sh1-PaloAlto)
AdventureWorks2014-SPO	Direct	Silver (sh1-Stuttgart)
AdventureWorks2014indo	Direct	12hr-30d-AWS (sh1-PaloAlto)
AdventureWorks2016	Unassigned	No SLA
AdventureWorks2016	Derived from SQLEXPRESS2016	MSSQL-1d-30d-NoArchive
AdventureWorks2016stutest	Derived from MSSQLSERVER	6hr-30d-Azure (sh1-PaloAlto)
AdventureWorks2017	Direct	12hr-30d-AWS (sh1-PaloAlto)
AdventureWorks2019	Direct	12hr-30d-AWS (sh1-PaloAlto)
Cork	Derived from MSSQLSERVER	MSSQL-1d-30d-NoArchive
cowboys	Direct	MSSQL-1d-30d-NoArchive
DBAAdmin	Derived from MSSQLSERVER	MSSQL-1d-30d-NoArchive

The RSC SQL Database Dashboard allows you to monitor the SLA Domain assignments and inheritance for all hosts, instances, databases, and AGs.

Protecting a Windows Failover Cluster Instance (FCI) is just as easy as protecting a single host with Rubrik. By assigning the Service Level Agreement (SLA) Domain at the Windows Cluster level, all instances within the cluster will inherit the same SLA Domain, and consequently, all databases within those instances will also inherit the same SLA Domain. Additionally, you can assign an SLA Domain to a specific database for exceptional management, just like you would with a stand-alone host.

In the case of an FCI, Rubrik will automatically detect any instance failover and adjust accordingly without any reconfiguration. This means that backups will continue without any need for user intervention

To protect an Availability Group, all replica servers must be registered with Rubrik. Once the auto-discovery process is complete, you can assign an SLA Domain to the host, which will ensure the protection of all databases on the server that are not part of an Availability Group. As you add new databases to the server, they will be automatically discovered and protected, and backups will occur without requiring any additional configuration from you.

To safeguard the group, the next step is to assign an SLA Domain to it. You can opt to use the same SLA Domain as the host or choose a different one. Once the SLA Domain is assigned to the group, Rubrik will automatically protect all databases within the group. Moreover, it will also identify and protect any databases added to the group in the future.

It's the DBA's responsibility to create the Availability Group and configure the backup preferences. Rubrik follows these preferences and conducts the database backup on the replica server specified by the backup preferences. In the event of an AG failover, Rubrik adjusts accordingly without any user involvement, as it checks the backup preferences every time a backup is executed and switches to the appropriate replica server.

In general, more intricate environments will follow the fundamental principle of "Protect the host, Protect the group." However, the application of this principle may vary based on the level of complexity involved.

OPTIMIZED DATABASE PROTECTION

Now that you have reviewed how Rubrik manages data protection in a SQL Server environment, let's dive into the nuts and bolts of how Rubrik takes a backup. Due to the wide variety of database sizes, densities, and configurations, there are a number of key highlights or techniques Rubrik uses for optimized backup.

VSS WRITER

Rubrik leverages the Microsoft-provided SQL Writer Service, as well as Rubrik's Scalable Snapshot Service, depending upon the given workload. These services use the Volume Shadow Copy Service (VSS Writer) to freeze I/O on the database (also known as quiescing the database), which allows Rubrik to take a read-consistent snapshot of the SQL Server files. The process is as follows:

1. Rubrik freezes the I/O of the target database using VSS.

   Note: Since IO is only frozen for the target databases, the impact on the workload is minimized.

2. A filesystem shadow copy is generated with database files in their consistent state.

3. I/O is thawed so that database operations can continue.
4. Rubrik begins copying the shadow copy of the files to Rubrik's immutable file system as a snapshot.

While all backup actions are recorded in the `msdb.dbo.backupset system` table, SQL Server only records the time that the VSS shadow copy is made. Because the I/O freeze and thaw operations are typically 1-2 seconds, that is the time recorded by VSS for the backup operation.

The Scalable Snapshot Service developed by Rubrik accommodates vertically-scaled instances of SQL Server (1,000+ databases) by reducing the overhead of job handling vs. the Microsoft-provided SQL Writer Service. This feature can be enabled for a subset of databases, or an entire instance.

Once the VSS operation is complete, SQL Server does not track the completion of the Rubrik backup. To avoid false positives and ensure successful backups, refer to the backup status reported in RSC.

DATABASE BATCHING WITH VSS

While the above VSS example depicts the backup process for a single database, customers often have multiple databases residing on a single host or instance. For this reason, Rubrik designed an intelligent batching process to capture multiple databases in a single snapshot.

Multiple database objects are grouped together based on their associated SQL host and SLA domain through a single VSS operation. A batch job can contain up to 16 databases or a total of 1TB of databases, and if a database size is close to or greater than 1TB, the batch job will include only this single large database. This technique efficiently uses SQL host resources and speeds up the backup workflow. Additionally, it enables Rubrik to perform multi-select on-demand backups. To avoid excessive utilization of the CPU, storage, and network bandwidth on the SQL server host, Rubrik restricts the number of batch jobs that can run concurrently on a single host to three.

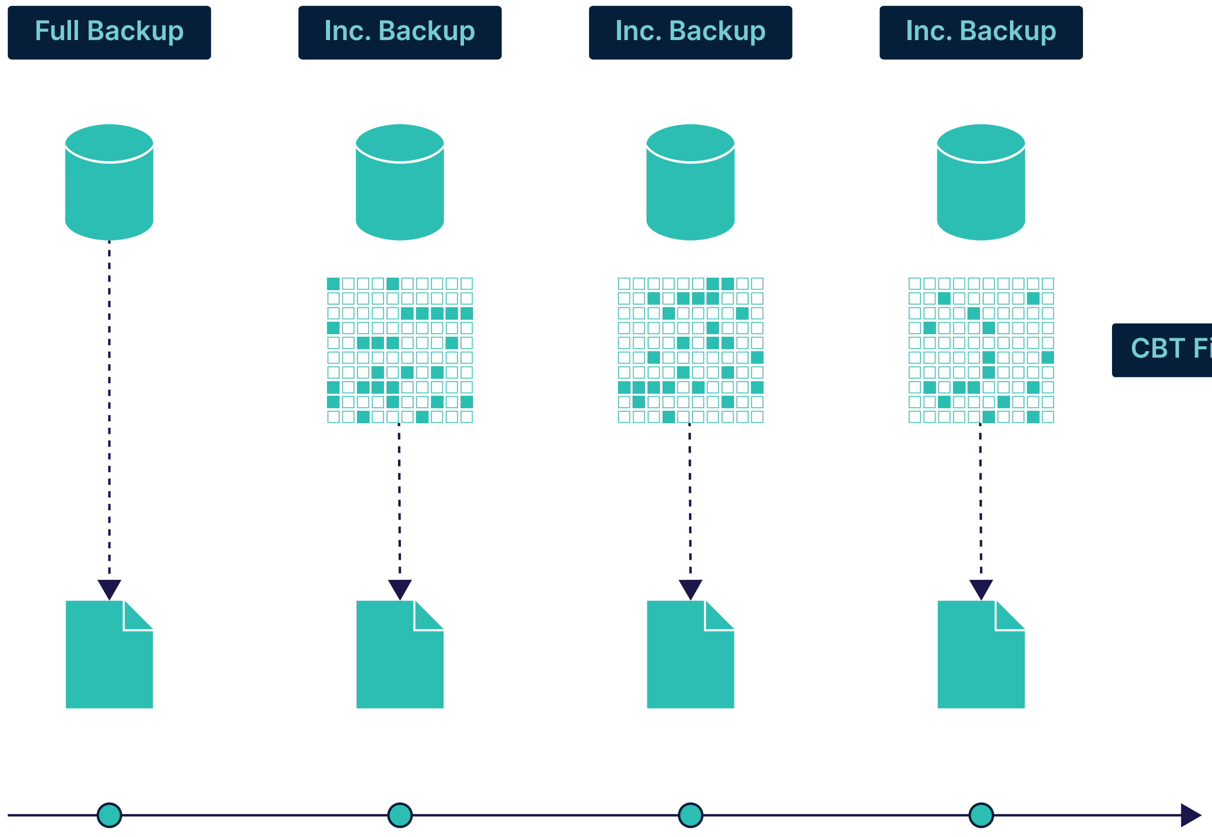
NOTE: While the database backups are grouped in the batch workflow, individual database backups are stored by the Rubrik cluster upon ingestion. This approach allows for a granular and efficient recovery, replication, and archiving operations.

INCREMENTAL FOREVER SNAPSHOTS

Incremental forever snapshots dramatically reduce storage usage and network traffic both inside the data center and over replication links. Although SQL Server does not natively support incremental-forever backups, Rubrik can provide this capability via block mapping using CBT or VSS scan and fingerprint methods.

CHANGE BLOCK TRACKING

From a storage standpoint, SQL databases often have the most frequent change rates due to their transactional nature. Without a mechanism to track the underlying changes in the database since the last backup, a full backup copy would have to be transmitted after each run. To mitigate this, RBS performs a scan and fingerprint of the VSS snapshot to identify the changed blocks. However, for larger individual databases (50GB or larger) or dense database deployments (many databases on a single host), Rubrik engineered a change block tracking (CBT) feature for SQL Server. When enabled, a lightweight filter driver is installed that actively tracks the underlying file operations on the database files. These changes are stored in a small file (64MB) in memory called a bitmap. When subsequent backups are taken, Rubrik reads from the bitmap file to quickly retrieve the changes since the last backup. This increases performance and circumvents the default behavior of scanning and fingerprinting the VSS snapshots.



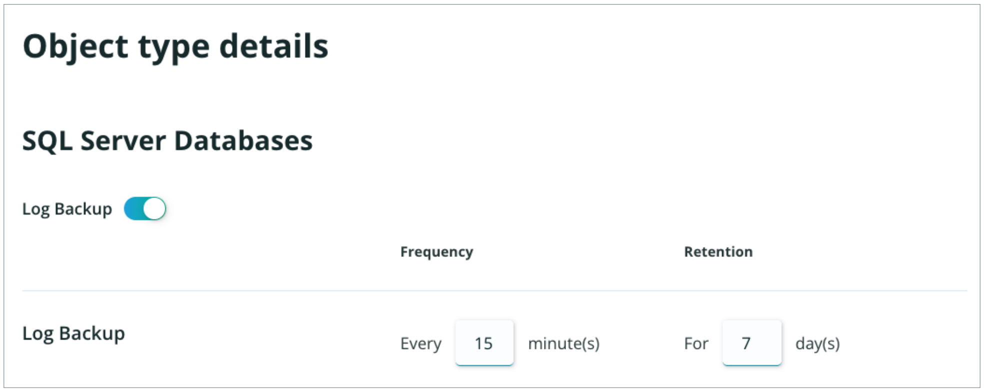
CBT can be enabled or disabled at the host level. The use of CBT is transparent and is determined by Rubrik, depending upon the size (50GB or larger) of the individual database. It is fully supported for Standalone, AGs, and Failover Cluster Instances.

Summarizing some of the caveats:

1. CBT is only effective for databases that are 50GB or larger.
2. Each host requires 64MB of memory, which is shared among all the database instances on that host. This allocation can monitor up to 32TB of changes.
3. CBT sessions are reset whenever the host is restarted, or there is an AG/FCI failover. When the session is reset, the next snapshot duration will be the same as the standard incremental forever snapshot.

SQL TRANSACTION LOG BACKUP

For databases in the Full Recovery model, Rubrik supports the backup of SQL transaction logs. The frequency and retention of the transaction log backups are configurable through the SLA Domain Policy that is assigned.



Object type details

SQL Server Databases

Log Backup ●

	Frequency	Retention
Log Backup	Every 15 minute(s)	For 7 day(s)

Similar to the application of an SLA Domain Policy, this feature gives you a simple method to ensure granular database protection across the deployment. If a database is configured in the Simple Recovery model with the same SLA applied, Rubrik will perform database backups as specified in the SLA. If transaction logs are handled by another process or system, the Copy Only mode can be used, and the transaction logs will be left untouched.

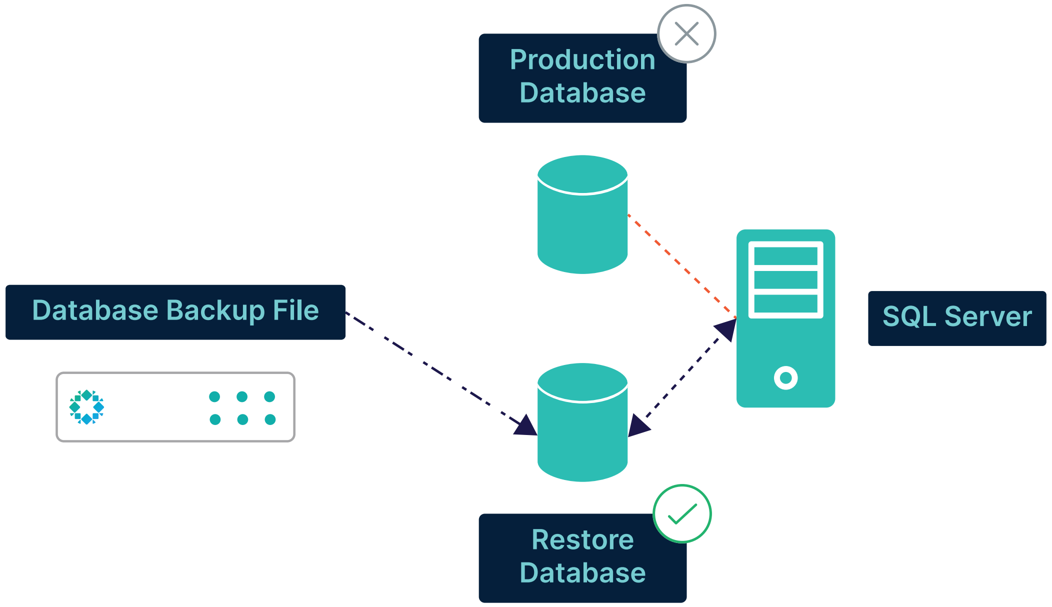
The combination of database snapshots and transaction log backups permits the granular restore of a database to a specified recovery point. See the Additional Features and Use Cases section below for details.

EXPEDITED RECOVERY BEST PRACTICES

Now that we have covered how Rubrik can manage SQL Server in various server and database configurations, let’s take a closer look at the available recovery options. The simplicity of Rubrik extends to the recovery operations.

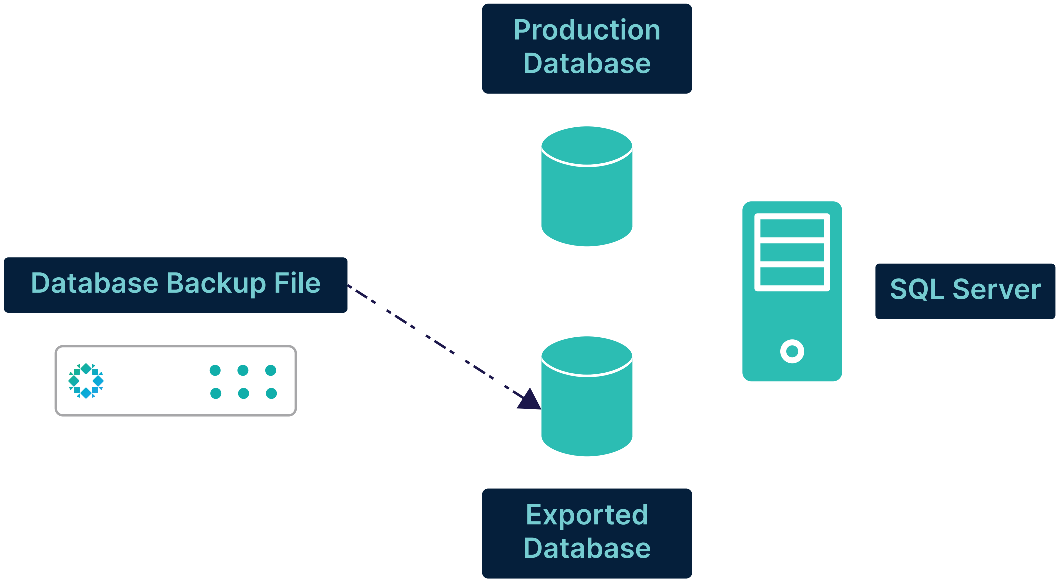
RESTORE

Choosing *Restore* drops the original database and creates a new database on the same instance with the same name and file structure. A common use case for this option is when a database is corrupted, and a restore to a previous point in time is desired.



EXPORT

Choosing *Export* creates a new database, and the existing database is not overwritten. If restoring to the same SQL instance, a different database name is required, with the file structure reflecting that name. The same or different database name can be used if the Export operation is in a different SQL instance. A common use case for this option is to use a production database snapshot as the source to clone a copy for test or development.

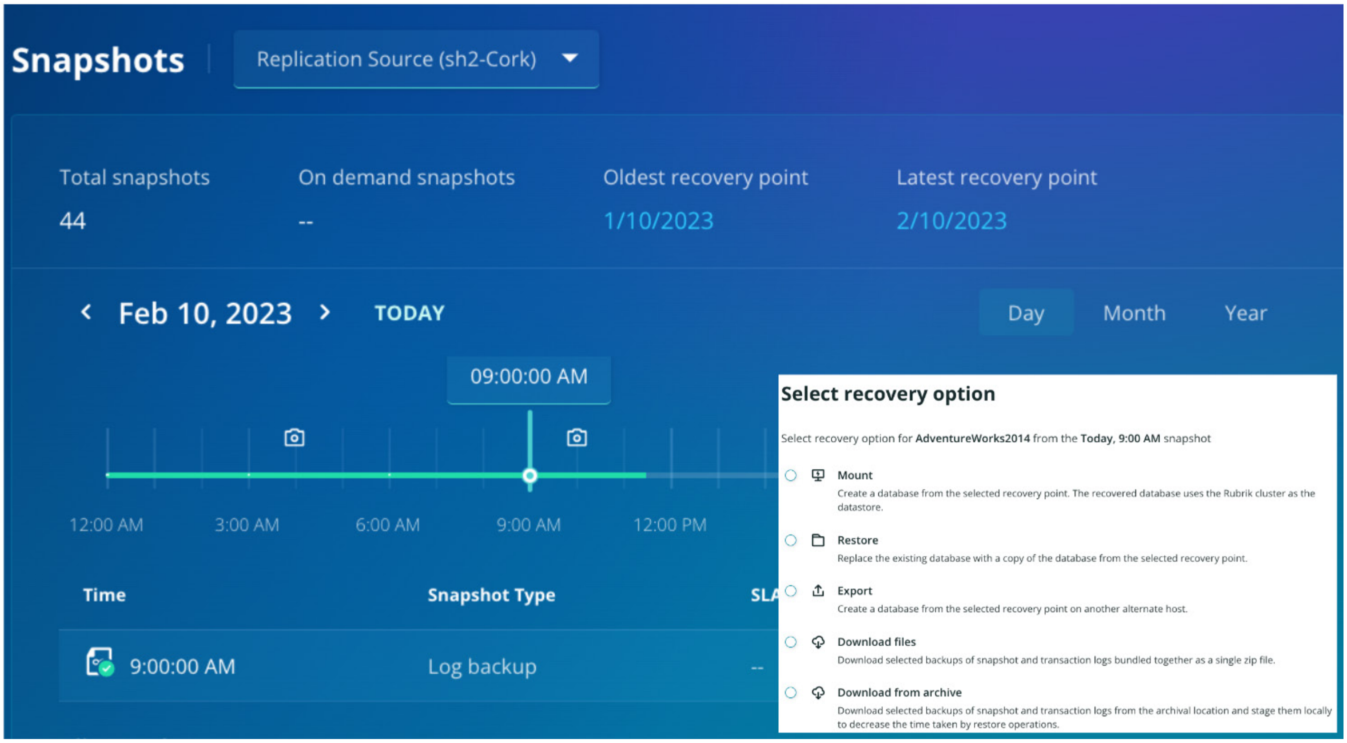


CROSS VERSION RECOVERY

SQL DBAs often need to restore SQL backups to different versions of SQL Server, whether for testing or restoring old backups where only newer SQL Server versions remain in the customer environment. Rubrik supports restoring databases to the same or newer SQL Server version. For precise details, please consult the Rubrik Compatibility Matrix for a current list of supported Source and Target SQL Server versions.

POINT-IN-TIME RECOVERY

SQL Server databases often require flexible recovery options. Since Rubrik is transaction log aware, performing point-in-time recoveries is possible. During the restore process, the Administrator specifies the desired restore time by selecting which day to recover from and then dragging the slider to the recovery point.



Total snapshots	On demand snapshots	Oldest recovery point	Latest recovery point
44	--	1/10/2023	2/10/2023

Time	Snapshot Type	SLA
9:00:00 AM	Log backup	--

Select recovery option

Select recovery option for **AdventureWorks2014** from the **Today, 9:00 AM** snapshot

○ **Mount**
Create a database from the selected recovery point. The recovered database uses the Rubrik cluster as the datastore.

○ **Restore**
Replace the existing database with a copy of the database from the selected recovery point.

○ **Export**
Create a database from the selected recovery point on another alternate host.

○ **Download files**
Download selected backups of snapshot and transaction logs bundled together as a single zip file.

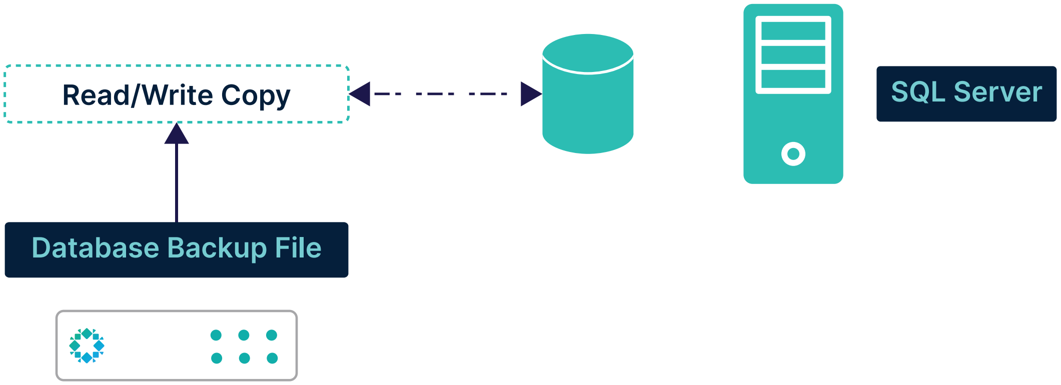
○ **Download from archive**
Download selected backups of snapshot and transaction logs from the archival location and stage them locally to decrease the time taken by restore operations.

The system then performs the following steps:

- Restores the full snapshot before and closest to the user-specified time.
- Transaction logs are then copied and replayed from the point of the snapshot to the time specified by the user, a process known as *rolling transaction logs*.

LIVE MOUNT

SQL Server *Live Mount* is an exciting technology that enables near-instantaneous recovery for databases running on physical and guest OS installations of Windows Server in a virtual environment. Administrators can Live Mount the database to recover a single table rather than completing a full restore to recover a portion of the data. The database files are hosted directly on the Rubrik cluster via a secure SMBv3 share.



The Live Mount is a read/write version of the database, allowing the user to manipulate the Live Mount as a normal database. Since the actual backup is immutable, it remains unmodified. This allows for quick access to the database for various use cases, which is discussed in the next section.

ADDITIONAL RECOVERY USE CASES AND FEATURES

This section explores additional features and use cases for the recovery of SQL Server. It covers a range of topics, from automation use cases to log shipping configurations with Rubrik.

LIVE MOUNT

Some fairly common and very unique use cases can be built around Live Mount. Let's discuss some of them.

Backup Validation

As backup administrators, you recognize the importance of testing all backups. Failure to do so can result in corrupted backups or applications failing to operate as expected post-restore. The only way to avoid any failures is to test your backups via a restore. With Rubrik, during the backup time, each block that is written is validated upon write. Ensuring that what was read, was written and nothing was corrupted during that process. On every database backup, a RESTORE VERIFY is done. You can also use the Rubrik Backup Validation APIs to read a backup and check if the backup is good. This is like RESTORE VERIFY ONLY with T-SQL. You can always use Export from Rubrik to create the database on another server. Those options are great and should be used, but they will all require time and resources. Depending on the size of the backup, this could be hours.

With Live Mount, you can restore the database quickly. Rubrik issues a restore operation via the SQL Server VSS Writer but keeps all the data on Rubrik, which expedites the entire validation process.

DATABASE CONSISTENCY CHECKS (DBCC)

You will often run DBCC to ensure that a database is free of corruption. These checks, however, come at the cost of production, compute resources, and administrative overhead. With Rubrik, you can simply use the API or pre-built SDKs to automate a DBCC check from a SQL Live Mount. Additionally, this automated process can be monitored systematically to send daily status reports or notify the DBA of corruption picked up by the process. Performing a DBCC CHECKDB on the Live Mounted database can determine if the backup contents are corrupt.

It is recommended to run DBCC CHECKDB on live databases as a best practice to ensure the production database is not corrupted. However, it is important to note that this process only confirms the contents of the backup.

Object Level Recovery

An eternal truth in the data center is that DBAs hate high RTOs. What is the recovery time for a 500 GB database? Or what about a 5 TB database? It is endlessly frustrating to wait for a full database restore when a DBA only needs to query or recover a few tables.

Given an immediate Live Mount, a DBA could selectively restore specific rows and tables via a simple ad hoc query, export, and import. This would provide far faster, and more granular database restore capabilities. Similarly, a database could easily be examined to track when specific data changed—there could even be multiple Live Mounts created to iterate back in time and pinpoint the exact time of a change. This may not be possible in a traditional environment, whether due to lengthy restores or not having extra disk space available for ad hoc requests.

Ad hoc scenarios are specifically enabled by the immediacy of Live Mount. Rubrik customers have found many variations on this theme based on the ease and speed of bringing a Live Mount online.

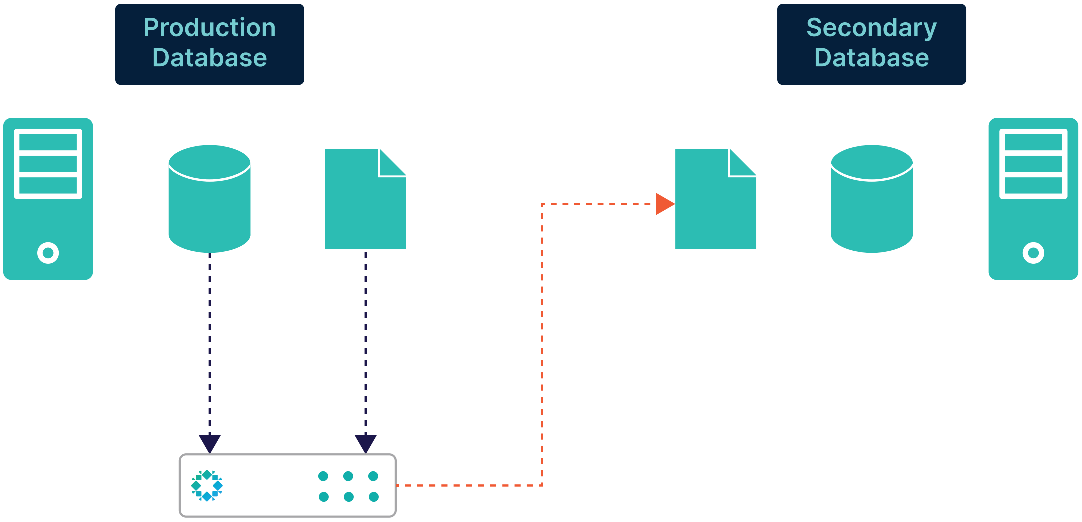
Testing and Development

Test and development environments are known for their volatility, with continual cycles of resetting the environment for application development. With SQL Server, a common task is restoring a database with seed data or production data.

Since Rubrik has an available API and SDK, it enables a simple way to integrate with existing automation tools. For example, backups can be called from the Rubrik API (or SDKs) in an Ansible Playbook during an environment build. Additionally, automating the refresh of multiple databases in the environment is a few lines of code away.

LOG SHIPPING WITH RUBRIK

SQL Log Shipping is a commonly used technique to provide an up-to-date secondary database copy, useful for disaster recovery. However, there are configuration steps needed with native SQL Server tools. With Rubrik, the DBA can simply add Log Shipping to the existing database being backed up and configure the secondary host, instance, and database. Once complete, Rubrik will automate the configuration tasks required on the primary and secondary SQL Servers.



ENCRYPTED DATABASE SUPPORT

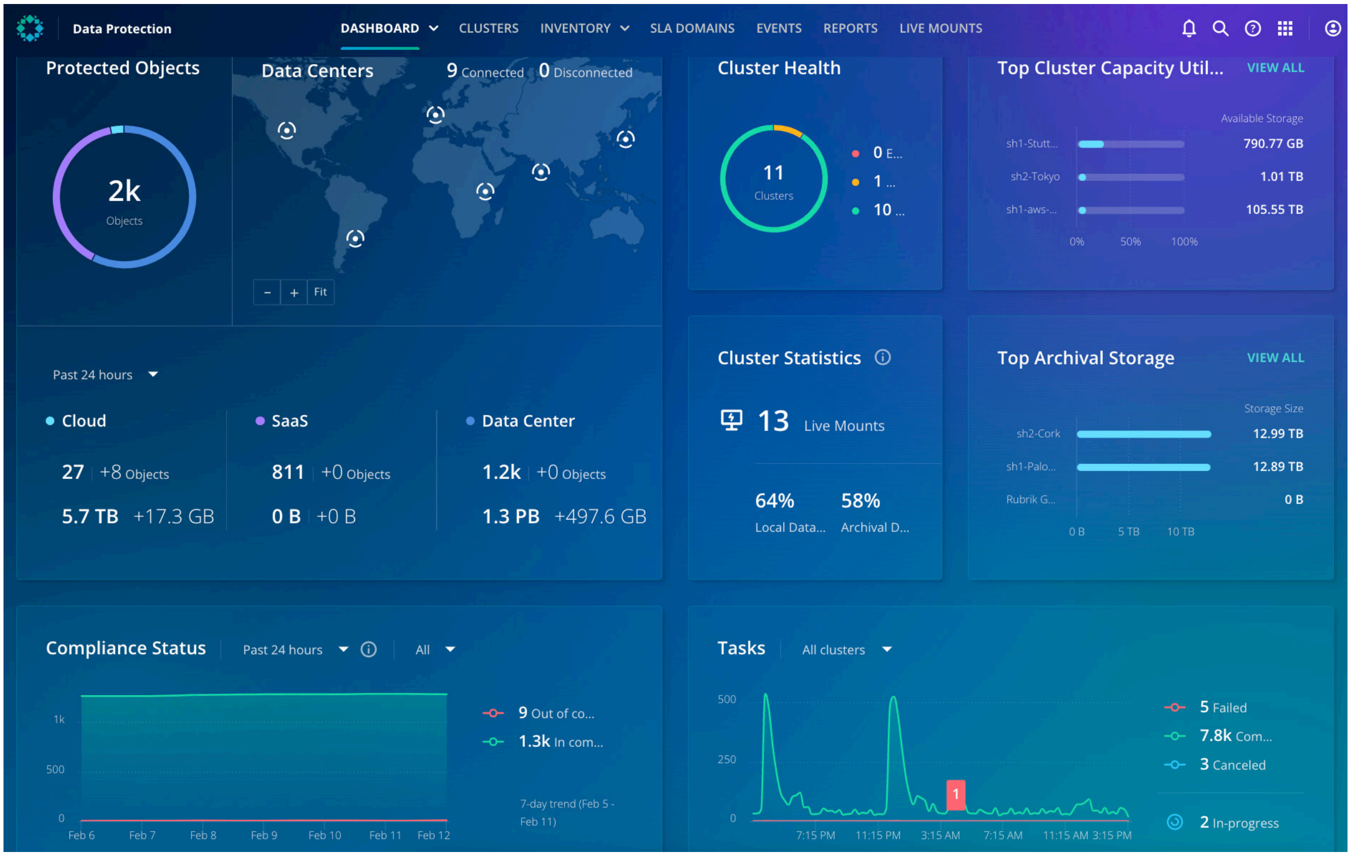
Rubrik can backup encrypted databases, and fingerprint-based compression will work on encrypted databases. For restore, the workflows are the same with one additional step—users must manage keys manually. The steps required to move keys are detailed in this Microsoft article. Once this is done, the intended database can be exported from the Rubrik UI.

CENTRALIZED MANAGEMENT AND REPORTING

Rubrik provides centralized management for your global, distributed Rubrik environment, focusing on delivering a seamless user experience. By providing a comprehensive view of your physical, virtual, and cloud topologies, Rubrik simplifies management tasks in an elegant and intuitive manner.

DATA PROTECTION DASHBOARD

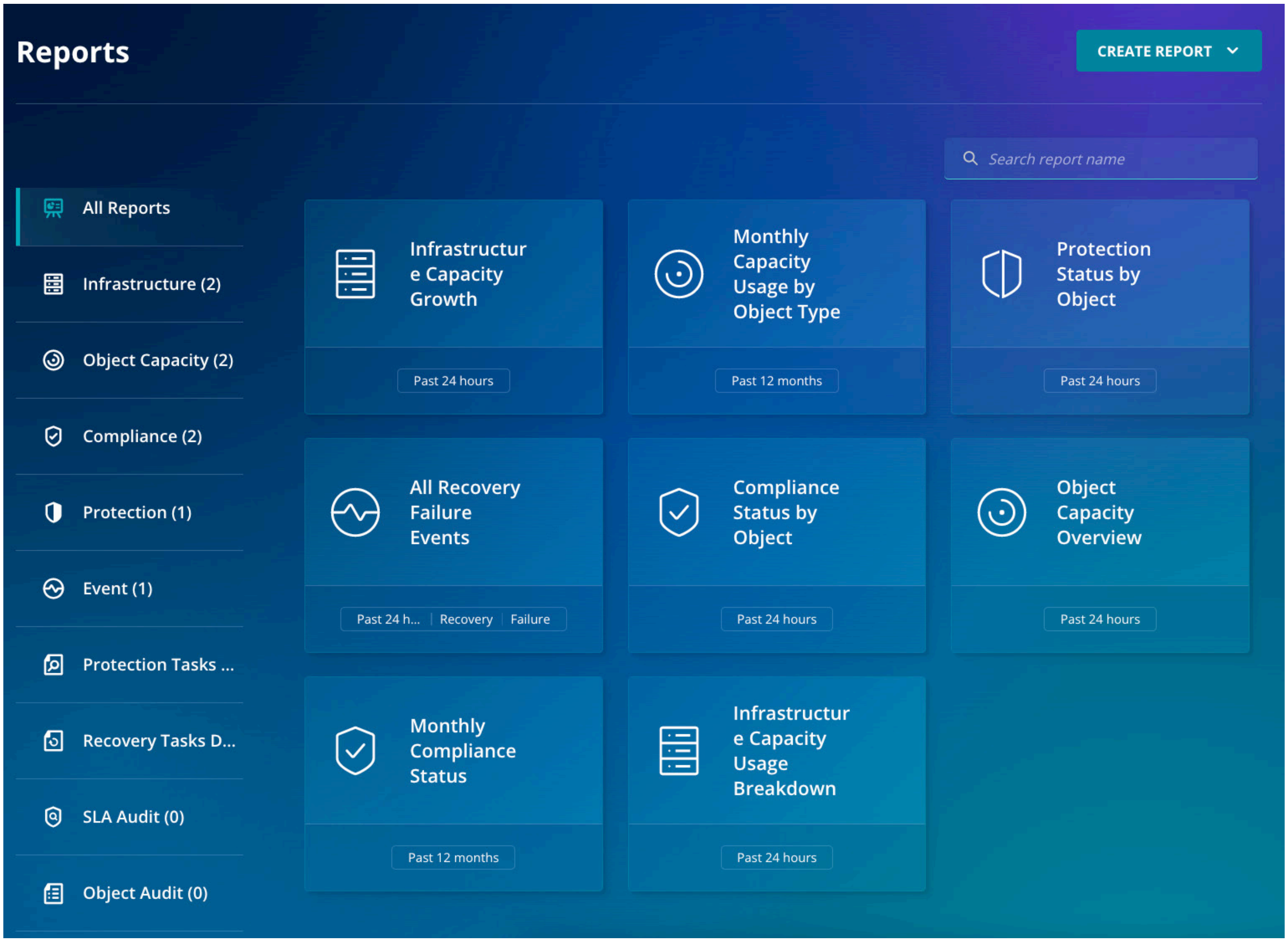
RSC includes the Data Protection Dashboard, which offers analytics on data management, compliance, and capacity utilization for your entire infrastructure—on-premises, at the edge, and in the cloud. This dashboard provides an at-a-glance view of SLA-compliant applications and enables you to display all set up events aggregated over a configurable time range.



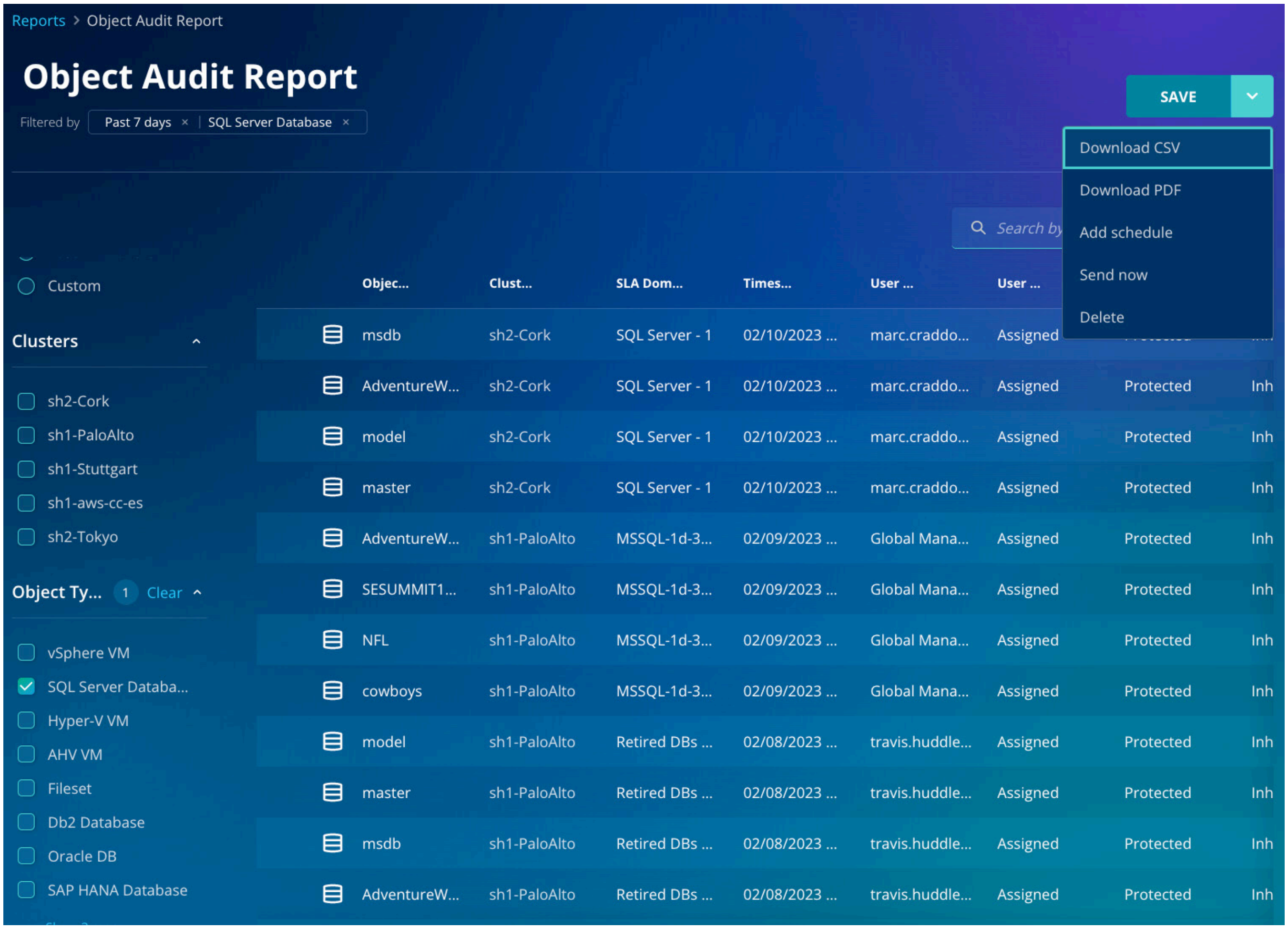
REPORTS

In addition, RSC offers reports that can be customized to display information on application data protection and the underlying infrastructure. Utilizing the on-demand infrastructure health and behavior insights allows you to maximize cost savings and performance while sharing rich data visualizations and customized reports that promote operational efficiencies.

Furthermore, a responsive HTML5-based interface enables the creation of custom reporting workflows using commonly used system metrics. The data collected in these reports can be used for audits and data management planning.



For example, RSC offers audit reports with granular historical information on SLA Domains and workload objects managed by Rubrik clusters to help with managing regulatory requirements . The SLA Audit report is generated by RSC once an SLA Domain is created, while an entry for the related details is added to the Object Audit report once an SLA Domain is assigned to a workload object such as SQL Server.



Reports > Object Audit Report

Object Audit Report

Filtered by Past 7 days × | SQL Server Database ×

○ Custom

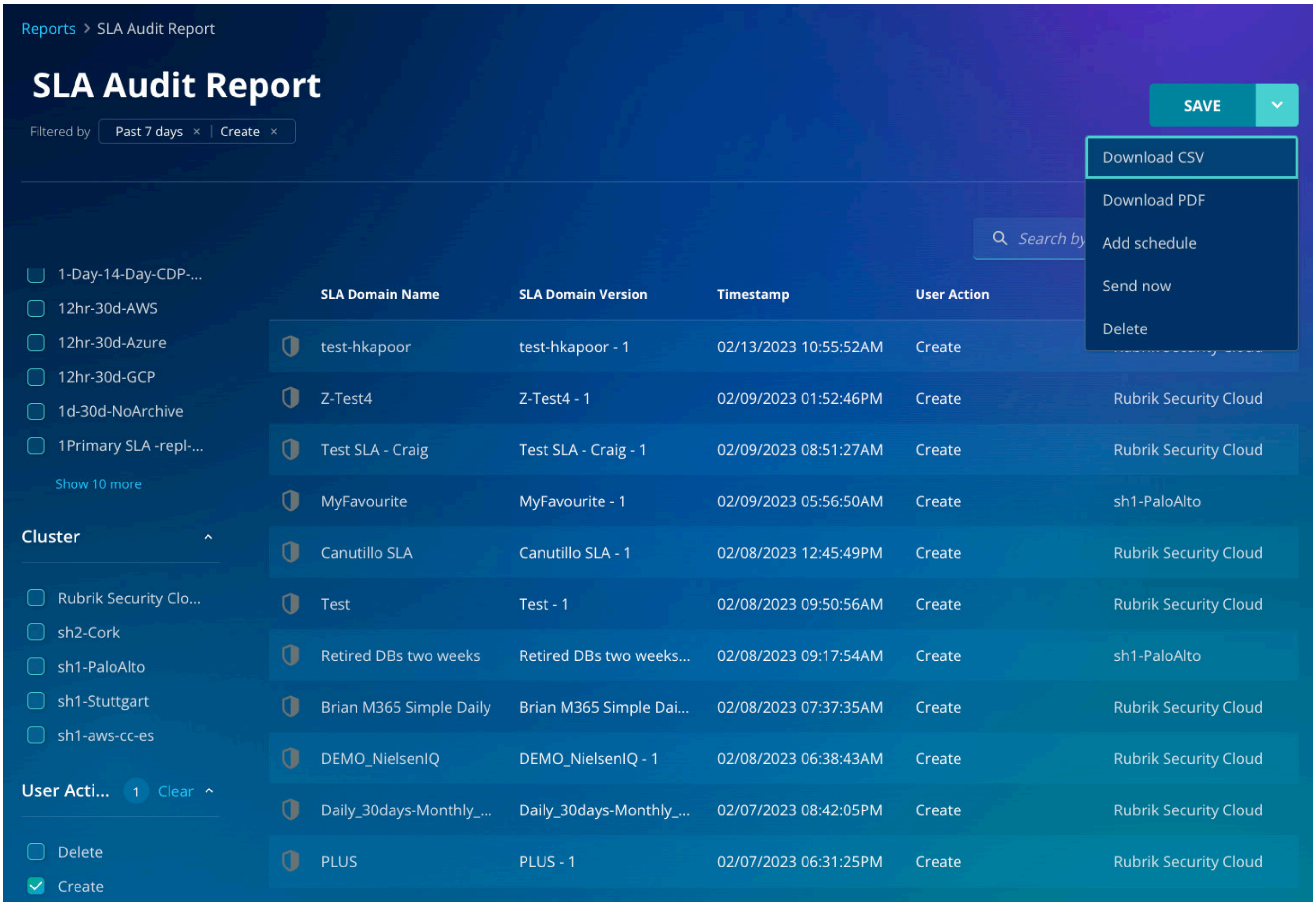
Clusters

- □ sh2-Cork
- □ sh1-PaloAlto
- □ sh1-Stuttgart
- □ sh1-aws-cc-es
- □ sh2-Tokyo

Object Ty... 1 Clear

- □ vSphere VM
- ☑ SQL Server Databa...
- □ Hyper-V VM
- □ AHV VM
- □ Fileset
- □ Db2 Database
- □ Oracle DB
- □ SAP HANA Database

Objec...	Clust...	SLA Dom...	Times...	User ...	User ...		
msdb	sh2-Cork	SQL Server - 1	02/10/2023 ...	marc.craddo...	Assigned		
AdventureW...	sh2-Cork	SQL Server - 1	02/10/2023 ...	marc.craddo...	Assigned	Protected	Inh
model	sh2-Cork	SQL Server - 1	02/10/2023 ...	marc.craddo...	Assigned	Protected	Inh
master	sh2-Cork	SQL Server - 1	02/10/2023 ...	marc.craddo...	Assigned	Protected	Inh
AdventureW...	sh1-PaloAlto	MSSQL-1d-3...	02/09/2023 ...	Global Mana...	Assigned	Protected	Inh
SESUMMIT1...	sh1-PaloAlto	MSSQL-1d-3...	02/09/2023 ...	Global Mana...	Assigned	Protected	Inh
NFL	sh1-PaloAlto	MSSQL-1d-3...	02/09/2023 ...	Global Mana...	Assigned	Protected	Inh
cowboys	sh1-PaloAlto	MSSQL-1d-3...	02/09/2023 ...	Global Mana...	Assigned	Protected	Inh
model	sh1-PaloAlto	Retired DBs ...	02/08/2023 ...	travis.huddle...	Assigned	Protected	Inh
master	sh1-PaloAlto	Retired DBs ...	02/08/2023 ...	travis.huddle...	Assigned	Protected	Inh
msdb	sh1-PaloAlto	Retired DBs ...	02/08/2023 ...	travis.huddle...	Assigned	Protected	Inh
AdventureW...	sh1-PaloAlto	Retired DBs ...	02/08/2023 ...	travis.huddle...	Assigned	Protected	Inh



SLA Audit Report

Filtered by: Past 7 days × | Create ×

- □ 1-Day-14-Day-CDP-...
- □ 12hr-30d-AWS
- □ 12hr-30d-Azure
- □ 12hr-30d-GCP
- □ 1d-30d-NoArchive
- □ 1Primary SLA -repl-...

Show 10 more

Cluster

- □ Rubrik Security Clo...
- □ sh2-Cork
- □ sh1-PaloAlto
- □ sh1-Stuttgart
- □ sh1-aws-cc-es

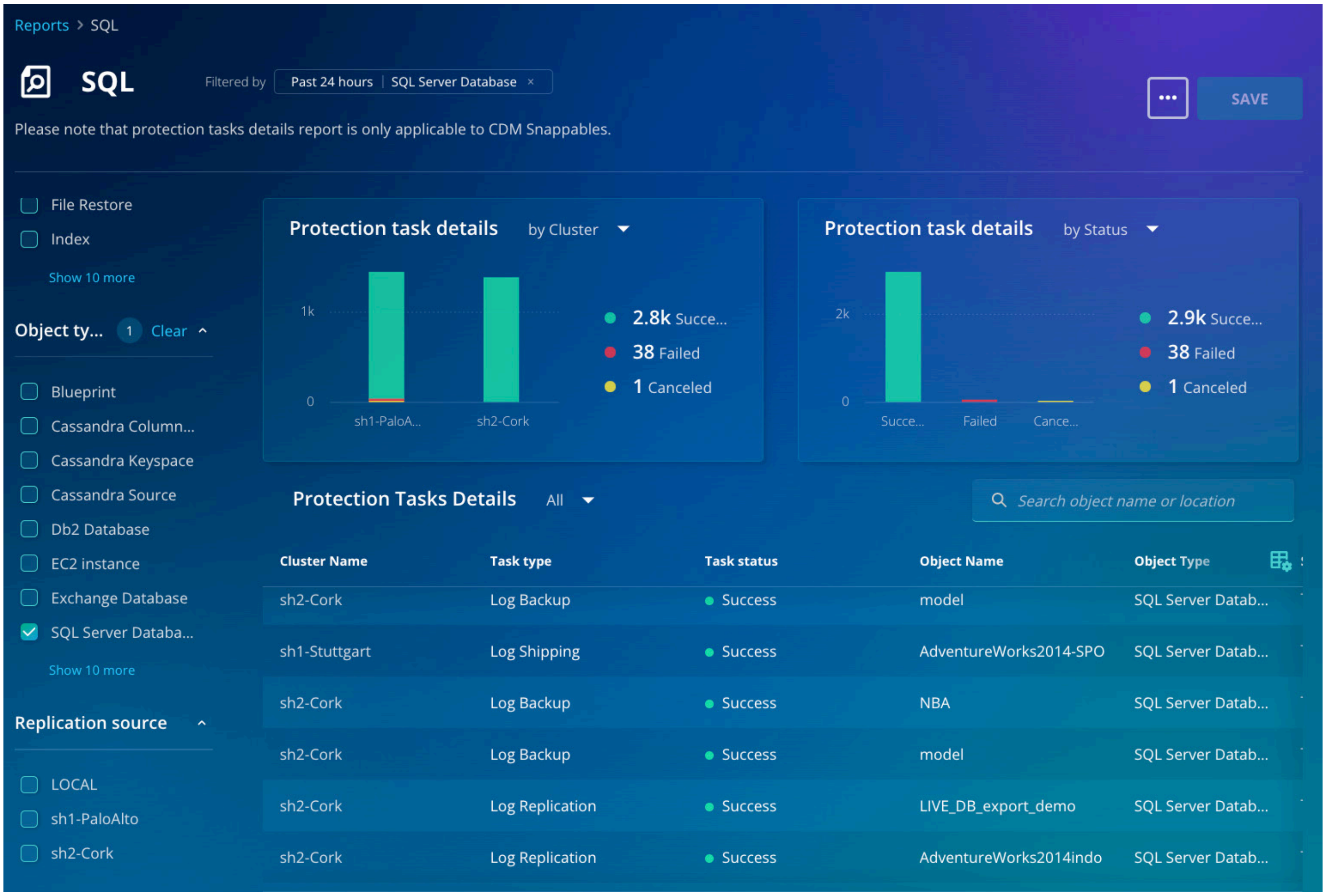
User Acti... 1 Clear

- □ Delete
- ☑ Create

SLA Domain Name	SLA Domain Version	Timestamp	User Action	
test-hkapoor	test-hkapoor - 1	02/13/2023 10:55:52AM	Create	Rubrik Security Cloud
Z-Test4	Z-Test4 - 1	02/09/2023 01:52:46PM	Create	Rubrik Security Cloud
Test SLA - Craig	Test SLA - Craig - 1	02/09/2023 08:51:27AM	Create	Rubrik Security Cloud
MyFavourite	MyFavourite - 1	02/09/2023 05:56:50AM	Create	sh1-PaloAlto
Canutillo SLA	Canutillo SLA - 1	02/08/2023 12:45:49PM	Create	Rubrik Security Cloud
Test	Test - 1	02/08/2023 09:50:56AM	Create	Rubrik Security Cloud
Retired DBs two weeks	Retired DBs two weeks...	02/08/2023 09:17:54AM	Create	sh1-PaloAlto
Brian M365 Simple Daily	Brian M365 Simple Dai...	02/08/2023 07:37:35AM	Create	Rubrik Security Cloud
DEMO_NielsenIQ	DEMO_NielsenIQ - 1	02/08/2023 06:38:43AM	Create	Rubrik Security Cloud
Daily_30days-Monthly_...	Daily_30days-Monthly_...	02/07/2023 08:42:05PM	Create	Rubrik Security Cloud
PLUS	PLUS - 1	02/07/2023 06:31:25PM	Create	Rubrik Security Cloud

You can download these reports in either CSV or PDF formats. Additionally, the report generation process can be automated. RSC can then send an HTML email containing the scheduled report, along with a CSV file containing the table data of the report, to all registered email addresses.

Another helpful report is the Protection Task Details category. This can be used to present the protection tasks for every cluster, along with a summary table containing more comprehensive details regarding your SQL workload.



Please note that protection tasks details report is only applicable to CDM Snappables.

Cluster Name	Task type	Task status	Object Name	Object Type
sh2-Cork	Log Backup	● Success	model	SQL Server Datab...
sh1-Stuttgart	Log Shipping	● Success	AdventureWorks2014-SPO	SQL Server Datab...
sh2-Cork	Log Backup	● Success	NBA	SQL Server Datab...
sh2-Cork	Log Backup	● Success	model	SQL Server Datab...
sh2-Cork	Log Replication	● Success	LIVE_DB_export_demo	SQL Server Datab...
sh2-Cork	Log Replication	● Success	AdventureWorks2014indo	SQL Server Datab...

Visit the RSC user guide to read more about all the options available as part of Reporting.

CONCLUSION

Rubrik delivers a comprehensive and automated data protection solution for your MS SQL databases while providing instant access with near-zero recovery time objectives (RTOs). Designed to manage all your physical and virtualized databases with a single, user-friendly interface, Rubrik can handle both on-premises and cloud environments. With fast object-level recovery and the ability to create unlimited database clones for application development purposes within seconds, Rubrik is an ideal choice for data protection and management.

NEXT STEPS

To learn more, check out our website or contact your sales representative.

VERSION HISTORY

Version	Date	Summary of Changes	Authors
1.0	March 2023	Initial Release	Alpika Singh, Jeff Inouye

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

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

rwp-protecting-microsoft-sql-server-with-rubrik / 20230328