**Rubrik Backup and Restore Documentation**

**1. Introduction**

This document provides an overview of backup and restore operations using Rubrik. Rubrik simplifies data management with an integrated approach to backup, recovery, and disaster recovery. This guide covers how to back up and restore data in a Rubrik environment, ensuring you can safeguard and recover your critical data.

**2. Prerequisites**

* **Rubrik Appliance**: Ensure that your Rubrik appliance is properly set up and running.
* **Kubernetes Cluster** (for Kubernetes workloads): Ensure that your Kubernetes cluster is properly configured and that Rubrik's Kubernetes integration is installed.
* **Access Credentials**: You must have administrative access or Group/Role based user access to the Rubrik system and necessary permissions for backup and restore operations.
* **Command Line Tools**: Ensure kubectl and any necessary Rubrik CLI tools are installed.

**3. Backup Overview**

**3.1. Concepts**

* **Backup**: The process of copying data to a secure location to prevent data loss. Rubrik performs incremental backups, capturing only the changes since the last backup.
* **SLA Domains**: Service Level Agreements (SLAs) define the backup schedule and retention policies. They ensure that data is backed up according to the specified policies.

**3.2. Backup Types**

* **Full Backup**: A complete snapshot of the data at a specific point in time.
* **Incremental Backup**: A backup that contains only the changes made since the last backup.

**4. Setting up Kubernetes Cluster Integration and Performing Backups/Restores.**

**4.1. On-boarding to Rubrik for Orbit Team or Orbit Kubernetes platform users**

* **Fill in the on-boarding form using** <https://jira.digital.ingka.com/servicedesk/customer/portal/181/create/1928>
* **Orbit Team:** Ensure you provide the cluster name and summary to get access to the entire cluster and all the namespaces within the cluster. Ensure to update summary with Azure AD group which needs to be provided with role-based access.
* **Orbit Platform Users:** This can be also requested via Orbit team. Ensure you provide the cluster name and only the namespace for your specific application with no access to Delete option for the role-based user. Ensure to update summary with Azure AD group which needs to be provided with role-based access.

**4.1. Integrating Rubrik Orbit Kubernates cluster**

* Rubrik doesn’t have the functionality to integrate or manage Kubernetes via CRDs. Rubrik engineering team is working on this functionality and will be available for users in near future. Till then Rubrik must be integrated and the backups/restore should be performed via Rubrik UI.
* Login to Rubrik UI <https://ikea.my.rubrik.com/datasource_settings/k8s> and click Add Kubernetes Cluster.
* Enter Kubernetes Cluster details, select Kubernetes Upstream for Kubernetes Distribution and select the Rubrik cluster as suggested by GStorage team where we need to backup our Kubernetes.
* Upload KUBECONFIG and click Add.
* The Kubernetes cluster should now be visible and should show as connected in Rubrik UI.
* On Kubernetes cluster we should be able to see rubrik-kupr namespace automatically created with resources running in it.

A screenshot of a computer screen

Description automatically generated

A close-up of a screen

Description automatically generated

A screenshot of a computer

Description automatically generated

**4.2. Configuring Protection Set to backup namespaces within the K8 cluster.**

* Login to Rubrik UI and navigate to Kubernetes section and click Protection Sets.
* Click Create a Protection Set, select the namespace to be protected and check the box to include all the resources in the namespace.
* Provide the protection set with a name (eg: - namespace-ns-ribrik) and create the protection set.
* Select the create protection set and click manage protection.
* Select an SLA domain as per backup requirement and assign the backup SLA Domain to the namespace/protection set.
* SLA Domain details can be found on <https://confluence.build.ingka.ikea.com/pages/viewpage.action?spaceKey=DATAPROTEC&title=High+Level+Data+Retention+Strategy>

A screenshot of a computer

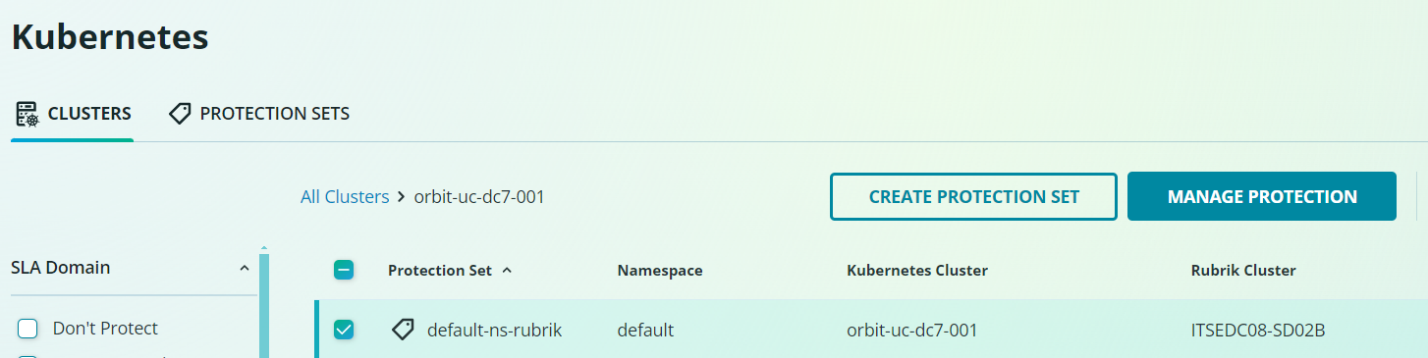
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**4.3. Perform restore using Rubrik.**

* Select the Protection Sets (namespace you want to restore).
* Select the date from which you want to restore.
* Select the option based on need, either restore entire protection set (namespace) or PVC or specific resource within the protection set (namespace).
* Perform backup recovery.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a recovery

Description automatically generated

A screenshot of a computer

Description automatically generated