

Rancher on AWS, Backup to S3 with IRSA for Authentication

Date: 2023-07-04
modified: 2023-07-12
tags: AWS, EKS, IRSA, IAM, Kubernetes, Amazon, Rancher, Backup, S3
description: Rancher Backup to S3 with IRSA
category: Container
slug: rancher-on-aws-backup-to-s3-with-irsa-for-authentication
Author: Dominik Wombacher
lang: en
transid: rancher-on-aws-backup-to-s3-with-irsa-for-authentication
Status: published

This is the second Article of the Series **Integrate Rancher with AWS services**, I'm going to demonstrate how to perform backups from Rancher to S3 by using IAM Roles for Service Accounts (IRSA) instead of EC2 Instance IAM Roles or AWS access keys.

Update: The recording of my talk [Rancher integration with AWS services: possibilities, challenges, outlook](#) (abstract and slide-deck) at openSUSE Conference 23 is online and covers parts of this article as well.

- media.ccc.de (includes options to download video and audio)
- youtube.com

Terminology	1
Kubernetes objects and annotations	1
Helm chart, repository, release	1
IAM Role and IRSA	1
Rancher Backup	2
Overview	2
IRSA Configuration	2
Conclusion	2

Terminology

Kubernetes objects and annotations

I assume you are aware what Kubernetes [objects](#) and [annotations](#) are, if not, that's your chance to brush up your knowledge, I will use these terms to explain the configuration of Rancher Backup.

Helm chart, repository, release

Again, I assume you are aware of [Helm](#) in general and also what a [chart](#), [repository](#) and [release](#) is. I'm going to use these terms later.

IAM Role and IRSA

To learn more about AWS IAM Roles and IRSA, I recommend to checkout the first Article of this series: [What is IAM Roles for Service Accounts \(IRSA\) and Amazon EKS Pod Identity Webhook?](#)

Rancher Backup

Overview

Rancher provides the [backup-restore-operator](#), it can be used to perform *scheduled* and *encrypted* backups of all Rancher resources. Amazon S3 is a supported target, which is a high available and resilient location for backups. IRSA can be used for authentication by adding the *serviceAccount annotation* during the installation.

The official documentation about [Backing up Rancher](#) provides further information about the functionality and general setup.

IRSA Configuration

The backup operator already supports IRSA but it's not covered in the official Rancher Documentation yet. It's sufficient to add three additional lines as part of the installation to activate it:

```
serviceAccount:
  annotations:
    eks.amazonaws.com/role-arn: arn:aws:iam::1234567890:role/my-rancher-backup-role
```

The complete values file for Helm could look like this for example:

```
s3:
  bucketName: my-rancher-backup-bucket
  credentialSecretName: ''
  credentialSecretNamespace: ''
  enabled: true
  endpoint: s3.us-east-1.amazonaws.com
  region: us-east-1
  serviceAccount:
    annotations:
      eks.amazonaws.com/role-arn: arn:aws:iam::1234567890:role/my-rancher-backup-role
```

Besides the *serviceAccount annotation*, the initial IRSA setup for the cluster and the creation of the IAM Role, with a link to the service account, used by the Rancher backup operator, is required.

The default service account name is `rancher-backup` in the namespace `cattle-resources-system`.

Further information can be found in [What is IAM Roles for Service Accounts \(IRSA\) and Amazon EKS Pod Identity Webhook?](#)

Conclusion

At first it was a little tricky to figure out if and how the Rancher backup operator supports IRSA, as I realized that the necessary code change was already merged a while ago, I was surprised, it's not mentioned in the documentation yet.

The actual configuration was then quite straight forward and similar as in examples I found in the [Amazon EKS documentation](#).

By default, long-term access key credentials are used by Rancher, which I would recommend to avoid, use short-term tokens as provided via IRSA instead, I outlined the *why* already in the first article of this series ;)

In the next article of this series, I will show you how to push log files from Rancher to CloudWatch and - again - to authenticate with IRSA instead of EC2 Instance IAM Roles or access keys.

1. [What is IAM Roles for Service Accounts \(IRSA\) and Amazon EKS Pod Identity Webhook?](#)
2. **Rancher on AWS, Backup to S3 with IRSA for Authentication**
3. [Rancher on AWS, Logging to CloudWatch with IRSA for Authentication](#)
4. Rancher on AWS, SAML Authentication with AWS IAM Identity Center as SAML IdP (coming soon)
5. Rancher on AWS, GitOps with Fleet and AWS CodeCommit (coming soon)