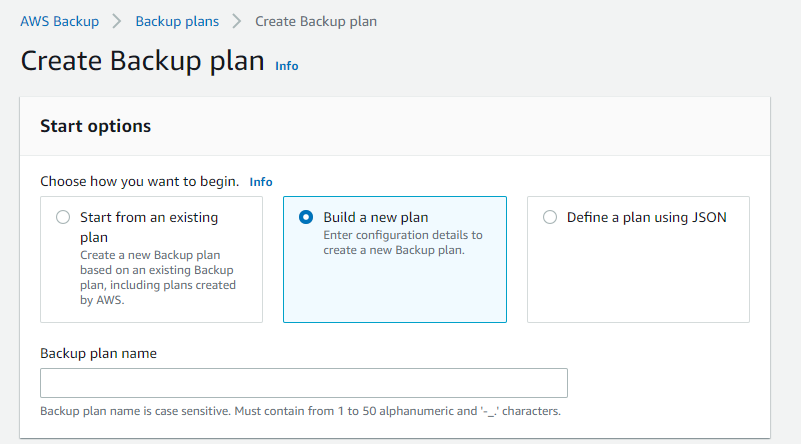
**AWS Backup Service**

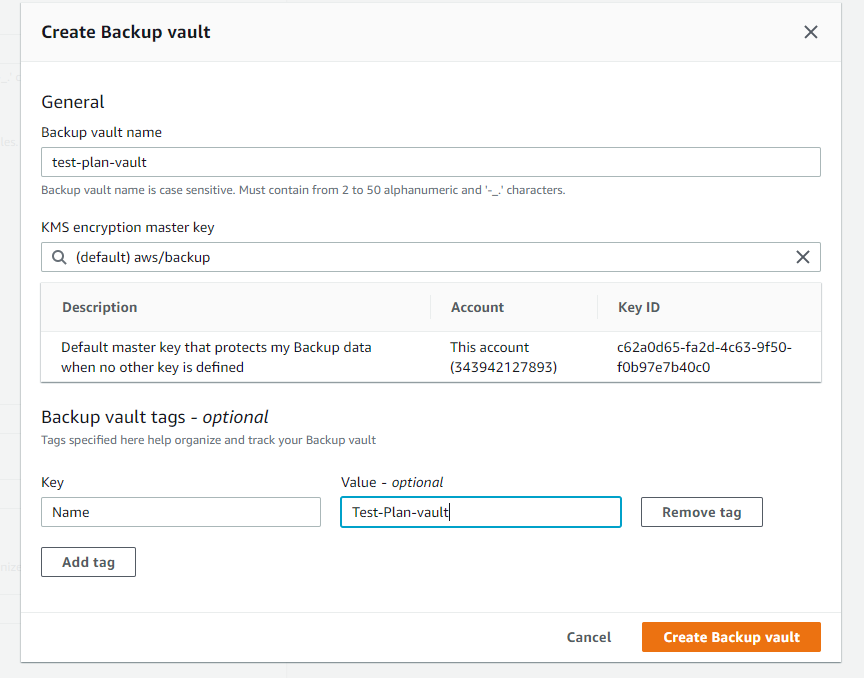
* Login to AWS console and search in the service “AWS Backup”
* Press “Create Backup Plan” and on next page choose “Build a new Plan” and give the plan a name.



* In the Backup Rule and configuration configure:

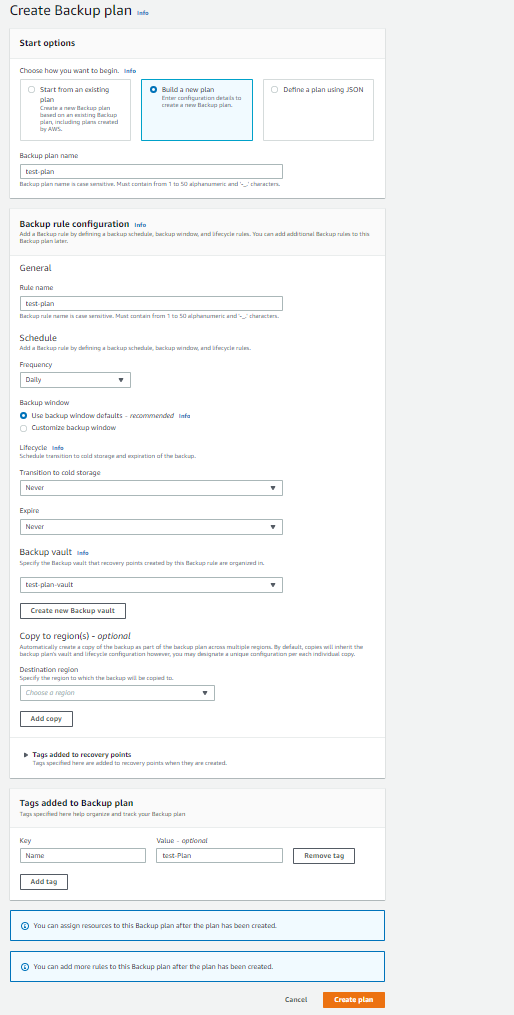
1. Rule name (can be same as plan name).
2. Frequency of backup (standard is daily).
3. We are using the default backup window unless needed a change
4. Transition to cold storage- **Never**
5. Expire- most cases :
   1. production is 14 days
   2. stage/PreProd is 7 days.
6. Backup Vault-
   1. create new one to match the naming convention of the backup plan
   2. encryption with the AWS “(default) aws/backup”,
   3. Define relevant Tags to Vault.

Example below:

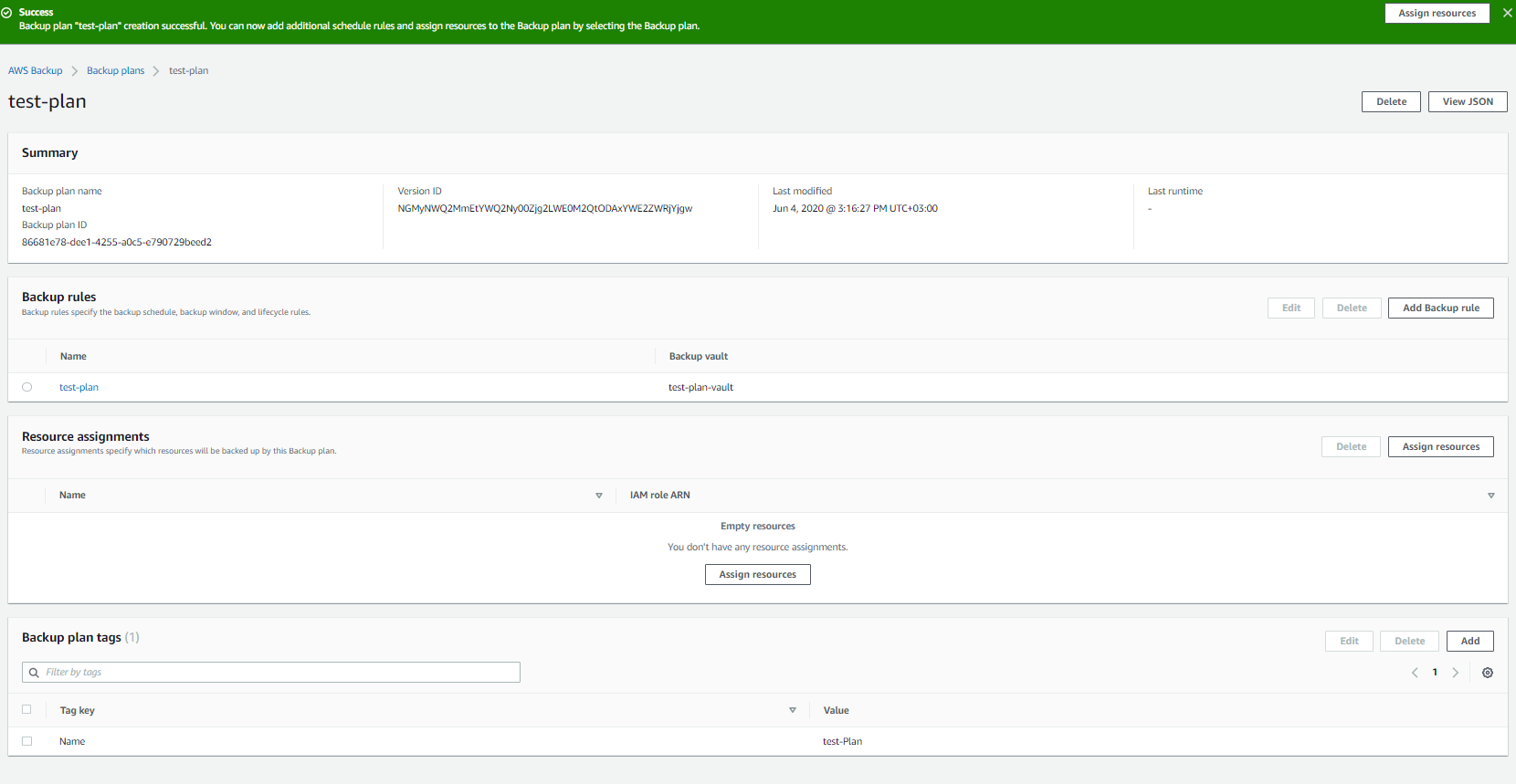


1. Copy to region- leave empty unless needed
2. If needed Tags for the recovery point add them (we do not configure it)
3. Add Name Tag to the backup plan

Example page below:

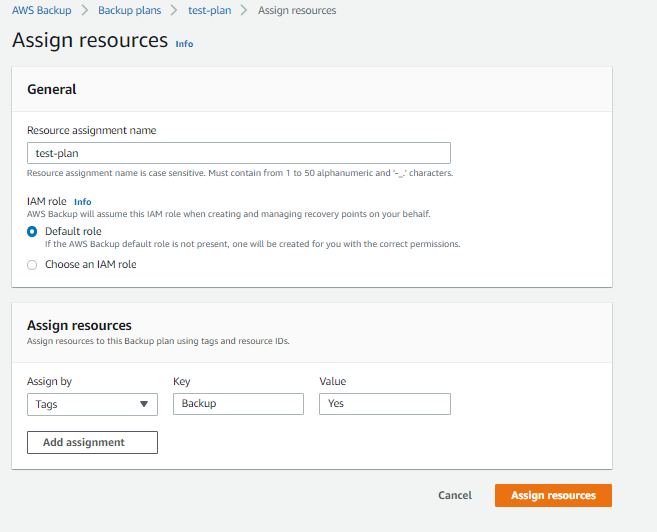


* Once backup plan is created go to the plan and you will see the following screen:



* Click on “Assign resources” and choose the resource assignment name (can be matching the name plan) and choose the TAG and value to add to objects in order for them to be backed up (TAGs for backup may be different between environments).

This is example page:



* Add policy to backup Role in order to be able to restore the instances:

Search in the IAM section under Roles the following Role: [AWSBackupDefaultServiceRole](https://console.aws.amazon.com/iam/home?#/roles/AWSBackupDefaultServiceRole)

Add inline policy named “IAMPassRole\_Policy” and edit it with the Json TAB and add the following to the policy:

{

"Version": "2012-10-17",

"Statement": [

{

"Action": "iam:PassRole",

"Resource": "\*",

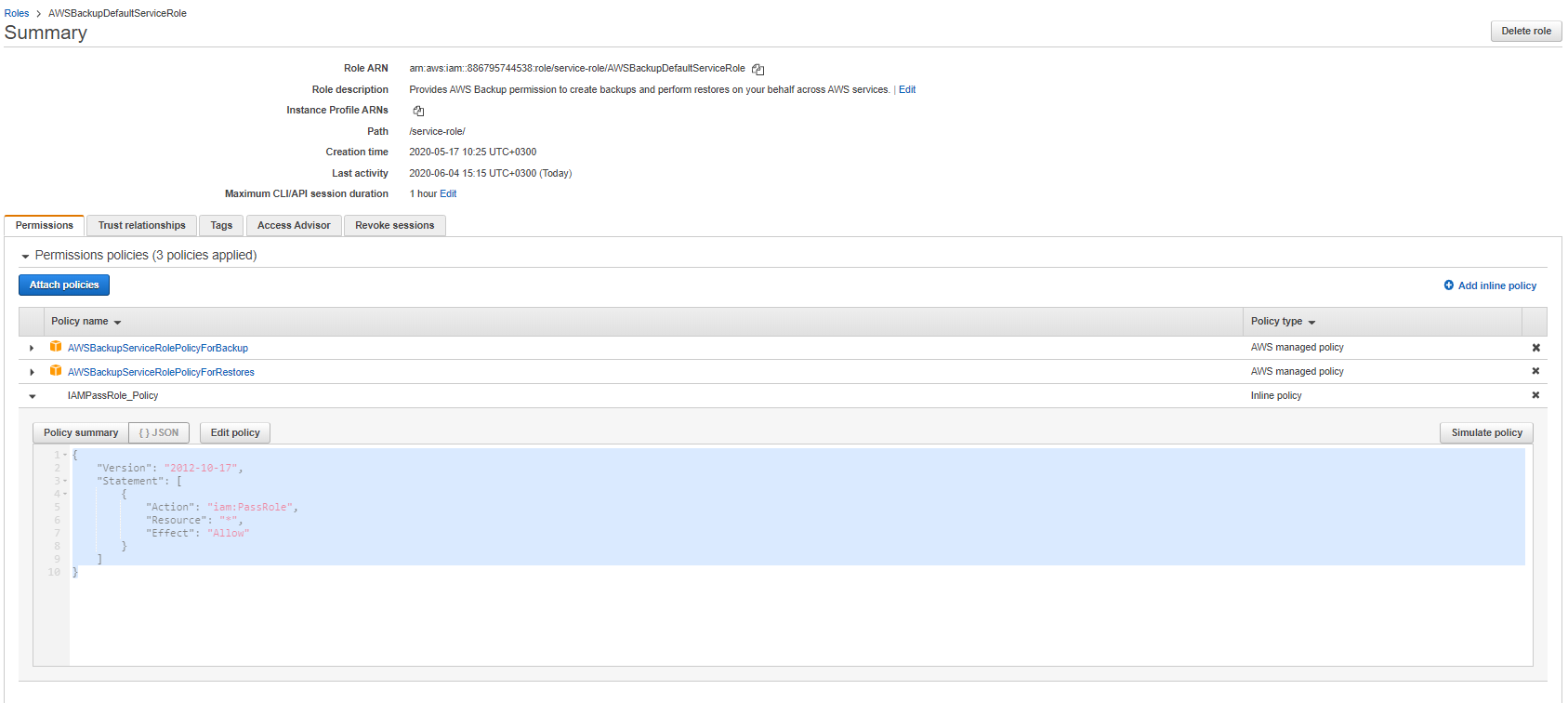
"Effect": "Allow"

}

]

}

It should be looked like that:



* Add the backup Tags configured to the relevant objects.