cloudcasa

Getting Started Guide for protecting Amazon RDS databases

1 Add your AWS account in CloudCasa

To be able to see and manage backups for your Amazon RDS databases in CloudCasa, you must first define your AWS account. As part of this process, you'll grant CloudCasa limited access to your AWS account, with just the minimum permissions necessary to manage backup and restore of your Amazon RDS databases (see our FAQ for the exact list of permissions). This is done using a CloudFormation template that CloudCasa supplies for you.

First, log in to CloudCasa, select the Protection tab, and select Accounts. Then Click "Add New Account".

Next, click the "Launch Stack" button. This will open another browser tab that will prompt you to sign in to AWS, and will then launch a CloudFormation stack that will grant CloudCasa the access it needs. Be sure to log in as an administrator so that CloudFormation can run.

Note: CloudFormation will create a stack called, by default, "cloudcasa-v010 ". That in turn will create a role with a name like "cloudcasa-v010-CloudCasaRole-XXXXXXXXXXXX". You can at any time, if you should so desire, remove CloudCasa's access to your account by deleting this stack.

When CloudFormation has completed, it will send a message back to CloudCasa, and your account configuration will be complete. This should only take a few minutes. You can then set a name for the account, if you wish. By default it will be set to your account number.

You can repeat this process multiple times if you have multiple AWS accounts to add.

cloudcasa

2 Define your backups

Once an AWS account is added, CloudCasa will automatically discover all of the RDS databases that account has access to. These will appear in the CloudCasa UI when you select “Databases” under the Protection tab.

Select “Databases” now, and click the “Define Backup” button in the upper right corner of the screen to start defining a database backup. The “Add new backup” pane will open, and you will be able to select one or more databases to include in your new backup definition. Click “Next” once you have chosen databases to proceed to the next page. Here you must assign a name to your backup, and optionally add key-value tags to help identify it. You can also enable the “Copy to another region” option if you wish to copy the snapshot(s) of your database(s) to another region. If you enable it, you must choose the destination region for the copy. You will also need to select a policy for the copy later in the process.

Next you’ll need to select a policy for your backup. If you are protecting a database that is part of a Kubernetes-based application, you may want to use the same backup policy that you use for the application’s namespace in Kubernetes. From this page you can also create a new policy, or select “None” if you don’t want to use a policy but only initiate backups manually. If you do select “None”, you can choose to enable the “Run now” option if you want to start an ad-hoc backup immediately. Note that if you choose “Run now” you will also need to choose a retention period for the ad-hoc backup.

If you chose a policy and selected the “Copy to another region” option earlier, you will next be prompted to choose a copy policy. Copies have their own policies so that they can run on a different schedule and/or have a different retention period than the original snapshot. Note that copy policies are not allowed to have an hourly schedule component. CloudCasa limits the frequency at which copies can run in this way because of AWS limitations that prevent a backup from happening while a copy is still in progress.

You can also choose whether or not to enable the “Delete snapshot after copy” option, which does exactly what its name states.
Now click “Confirm”, and your backup definition is done!

You’re done! That’s all there is to it!
Now you can sit back and relax,
knowing that your database is protected.

cloudcasa

A note about different types of RDS backups

Using CloudCasa, you can perform restores from three different types of RDS backups. These are snapshots created by CloudCasa itself (or the copies of those snapshots made to other regions), automatic backups done by AWS (if configured), and any manual snapshots taken through AWS.

When you define a scheduled backup or run an ad-hoc backup, CloudCasa takes what in AWS terms is a manual snapshot of the database. During restore, you will have the option of either restoring from a specific recovery point or to an arbitrary point in time. When restoring from a recovery point, you can select between restoring from an AWS automated snapshot (called "AWS Auto" in CloudCasa), a CloudCasa backup, or any manual snapshot that you've created previously on AWS (called "AWS Manual"). When restoring to an arbitrary point in time, you can specify any time between the last time the database transaction log was automatically backed up by AWS (approximately every 5 minutes) and the time of your earliest unexpired AWS automatic backup. So if the retention for AWS automated backups is 7 days, the allowed time range for a point-in-time restore for the database will be from less than 5 minutes ago to approximately 7 days ago.