

# cloudcasa Getting Started with CloudCasa™ Kubernetes Backup



Point your favorite web browser to [www.cloudcasa.io](http://www.cloudcasa.io) and create an account.

Just select **Sign Up** and fill in a few details. You can log in and start using CloudCasa right after verifying your email address. If you want to invite other users to join your organization, you can do that under Configuration/Users.

**Configure your AWS and Azure account(s) (optional)** If some of your Kubernetes clusters are in AWS or Azure, we recommend adding your cloud accounts under Configuration/Cloud Accounts. This will allow CloudCasa to auto-discover your EKS and AKS clusters, back up EKS and AKS cluster parameters, auto-create clusters on restore, and back up non-CSI EBS volumes on EKS.



Go to the Protection tab and add your cluster.

If your clusters were auto-discovered, you'll just need to find them in the Clusters list under your cloud account, in Configuration/Cloud Accounts and click on the install icon for each one. If not, you can add them manually by clicking Add cluster under Protection/Clusters Overview. Then enter your cluster name and description and click Register cluster.

Either way, you will see a cluster ID and a kubectl command to run that will install a lightweight agent on the cluster. If you are installing via our Helm chart or via a partner marketplace instead, make a note of the Cluster ID and follow the instructions specific to your installation method. Once installed, the agent will connect and register itself with the CloudCasa service, completing the process.



Create a backup policy by clicking **Add new** in the policies list.

A backup policy allows you to define when backups that use it will run and for how long they will be retained. You can have multiple schedules with different retention times in one policy. For example, a policy may specify the creation of hourly backups that are retained for 7 days, and daily backups that are retained for 30 days. Add or edit policies under Configuration/Policies.



Go to the dashboard and click **Define Backup**.

Enter the name for your backup and select your cluster. Choose what namespaces to protect and/or select resources by tag. Choose whether to create local snapshots of your PVs or copy them to CloudCasa's secure storage. By default, everything will be protected including PVs. Finally, select the policy to apply. If you create a backup with no policy, it will not run automatically but can be started manually on an ad hoc basis.

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