DATA SHEET

cloudcasa

CATALOGIC

CloudCasa - Kubernetes Data Protection and Application Resilience

Cloud-native backup-as-a-service or self-hosted that also supports multi-cluster management and monitoring of Velero.

Data Protection - Data Migration - Application and Cyber Resilience

Introducing CloudCasa™

CloudCasa is a powerful and easy-to-use backup service built for protecting Kubernetes, cloud databases, and cloud native applications. As a SaaS solution, CloudCasa removes the complexity of managing traditional backup infrastructure. With the new self-hosted option, get the additional security and control you need for an air-gapped or highly regulated environment. The rich feature set of CloudCasa simplifies and automates multi-cloud, disaster recovery and data migration with Any2Cloud recovery. Finally, CloudCasa helps you take cyber resilience to the next level by providing vulnerability scanning alongside traditional data protection services.

CloudCasa for Velero is a new service offereing that combines the simplicity and manageability of CloudCasa and its advanced cloud awarness with the benefits of Velero, the battle tested open-source Kubernetes backup tool. With multi-cluster and multi-cloud backup management capabilities added to Velero, users can do centralized configuration, monitoring and advanced cloud recovery, from the same CloudCasa dashbard.

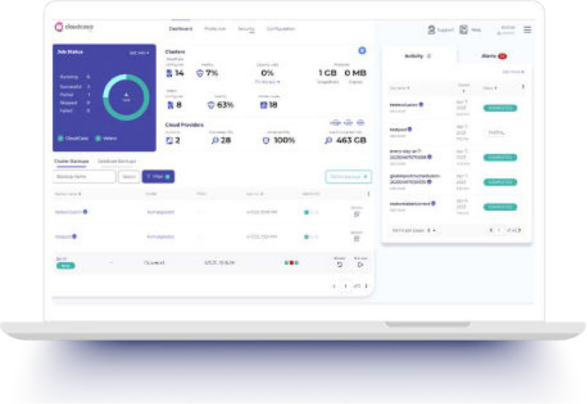
CloudCasa Highlights

- SaaS option requires no hardware or infrastructure to install and maintain.
- No hassle, and no backup expertise needed. Be up and running in 10 minutes.
- Self-hosted option for air-gapped and highly regulated environments.
- Securely encrypts data in transit and at rest.
- Manages protection for multi-cluster, multi-cloud and hybrid cloud environments with a single pane of glass.
- Open source compatible solution adds Velero backup management, including multi-cluster configuration, monitoring and guided recovery.
- Provides self-service backup with Clastic Capsule multi-tenant clusters.
- Supports all popular Kubernetes distributions including Red Hat OpenShift, SUSE Rancher and VMware Tanzu.
- Supports all popular Kubernetes cloud services including AKS, EKS, GKE, DigitalOcean, IBM Cloud, OKE, and OVHcloud.
- Protects cluster resources and presistent volumes.
- Enables cross-cluster, cross-account, and cross-cloud restores for migration and DR.
- Protects Amazon RDS datasheets and Aurora clusters.
- Cloud-aware integration for AWS, Azure, and GCP.
- IAM integration for enterprise single sign-on for both SaaS and self-hosted options.

CloudCasa Free SaaS Plan

Try our 100% totally free plan, no payment information required. The free plan includes:

- An unlimited number of clusters and worker nodes per account organization (limited to 15 nodes for Velero).
- Cluster resource data backups to secure cloud-based storage.
- Unlimited CSI snapshots of persistent volumes (PVs).
- Application hooks to trigger pre and post-backup and post-restore actions in your cluster.
- Protection of Amazon RDS databases, including scheduling and management of snapshots and point-in-time recovery*.
- Data retention period of up to 30 days*.
- On-demand vulnerability scanning of your Kubernetes and cloud account configurations*.
- Up to 3 user logins per account organization.
- Customizable role-based access control.
- Chat support and community support with active participation from the CloudCasa team.
- Limited time promotion to backup 100 GB of Persistent Volume data for free.



Does not apply to Velero clusters

CloudCasa Premium Plans

The CloudCasa for Velero plan includes all the features of the Free plan plus:

- Velero monitoring and alerts.
- Velero reporting and audits.
- Multi-cluster management with guided recoveries.
- Central log collection.
- Standard support with 99.9% SLA* that is upgradable to 24x7 support.

CloudCasa Pro plans include all the features of the Free and CloudCasa for Velero plans plus:

- Ability to back up PV data to CloudCasa with unlimited retention times*.
- Storage for backups is included in the plan. Included amount varies with Pro plans*.
- SafeLock with retention times to protection backups from being deleted*.
- Option to send backup data to your own object storage of choice.
- Scheduled vulnerability scanning of Kubernetes and cloud account* configurations.
- Unlimited user logins per account organization.
- API access for automation and CI/CD pipeline integration.

** SLA, included storage, SafeLock, and vulnerability scanning applies to SaaS version only.*

CloudCasa for Velero, CloudCasa Pro 1/5/20 TBs plans, and customizable Enterprise plans are available, with monthly or yearly subscriptions. Visit cloudcasa.io/pricing or contact us for pricing and further details.

CloudCasa Backup Storage

CloudCasa secure storage for SaaS is available in most AWS and Azure regions. You can select which provider and region each backup will be sent to. For Bring Your Own Storage for SaaS and self-hosting, the following object storage services have been tested and are supported: Amazon S3, Azure Blob, Backblaze B2, DigitalOcean Spaces, Google Cloud Storage, DataCore, Hitachi, OCI Object Storage, and Wasabi. Support for others is coming soon.

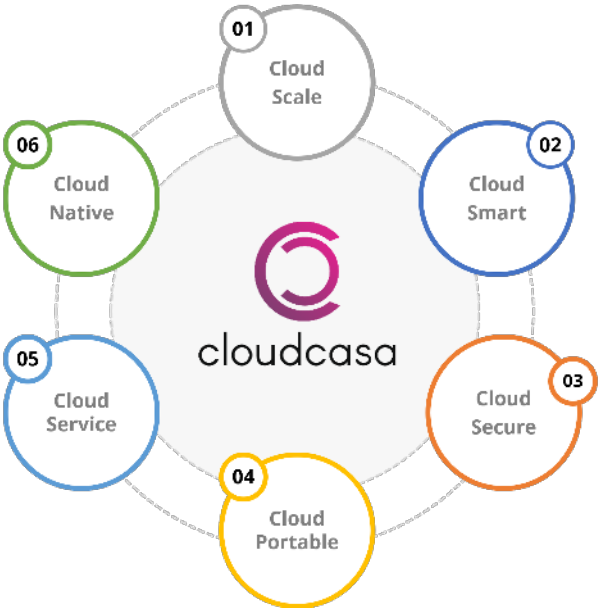
Why CloudCasa

Cloud Native
Built with Kubernetes for Kubernetes. Built in the cloud for cloud apps.

Cloud Service*
No Infrastructure and administrative burden.

* Self-hosted available

Cloud Portable
Enabling migration between platforms and cloud providers



Cloud Scale
Unlimited elastic storage and auto-scaling compute

Cloud Smart
Integrated with Big3: Azure AKS, Amazon EKS and Google Cloud GKE

Cloud Secure
Proactive scans + robust access + tamper- proofing + virtual airgap

CloudCasa Pro - Requirements and Compatibility

Software Requirements

- Kubernetes version 1.20 or higher for PV snapshots and backups
- Storage must use a CSI driver that supports volume snapshots
- Supports all popular Kubernetes distributions including: Red Hat OpenShift, SUSE Rancher, and VMware Tanzu
- Supports all major Kubernetes cloud services including: AKS, EKS, GKE, DigitalOcean, IBM Cloud, OKE and OVHcloud
- All Amazon RDS databases are supported, including Aurora
- Cloud-aware integration for AWS, Azure, and GCP accounts
- Clastix Capsule integration requires Capsule v0.1.0 or higher

Note: Just because a Kubernetes distribution or cloud service isn't listed here does not mean that CloudCasa will not work with it! Any variant of Kubernetes based on version 1.20 or higher should be compatible with CloudCasa. If in doubt, please contact our support.

Available Installations Methods

The CloudCasa Kubernetes agent can be installed using several different methods:

- Kubectl CLI method - Using custom YAML files available through the CloudCasa UI.
- Helm Chart - Available from our GitHub repository.
- OpenShift Operator - Available through the Red Hat OpenShift console.
- DigitalOcean 1-Click Application (https://marketplace.digitalocean.com/apps/cloudcasa)
- Via integration with many great partner products including SUSE Rancher, Rafay and Nirmata.

For self-hosted, the CloudCasa server installation is by Helm Chart, and the CloudCasa agent installation is by Kubectl CLI Method.

Permissions and Network Requirements for SaaS

The user configuring CloudCasa needs admin access to their cluster and access to the kubectl CLI, Helm utility, or other management console.

Network access from your cluster to the CloudCasa service (agent.cloudcasa.io on TCP port 443 is required. In addition, the object storage selected as a destination for your backups must be reachable from your cluster. No ports need to be opened for inbound connections.

The AWS login used to link your AWS account to CloudCasa for cloud-aware Kubernetes backup and restore, RDS backup and restore, and cloud vulnerability scanning requires administrative access, but the cross-account role created by our CloudFormation stack is limited to only the permissions necessary to perform required operations. Users have the ability to selectively include or exclude permissions for different features.

A similar scheme using Azure Resource Manager (ARM) is used for linking Azure accounts to CloudCasa. For GCP, a custom tutorial is used to walk users through the appropriate steps in Google Cloud Shell to grant CloudCasa the necessary access to a project using a custom role.