ProjectX

BACKUPS · DATASHEET

Retention tiers and cross-provider copies.

Backup policies with retention tiers and the option to copy a backup to a second provider — because a backup that lives only where the thing it protects lives is no backup when that place is the outage. Off by default where it doubles cost, on by an explicit choice.

Why teams choose it

01
Policy, not cron
Retention tiers decide how long each generation is kept, applied by the platform as policy — no scripts a person maintains and nobody forgets.

02
One outage cannot take both copies
An explicit durability flag copies a backup to a second provider, so the thing you protect and its backup are never lost to the same event.

03
Cost honesty by default
Cross-provider copies are off by default because they double cost — turning one on is an explicit, audited choice with the price consequence visible.

04
Restores from a recorded source
Every restore comes from a recorded backup, so recovery is a defined operation — not a search for whatever copy might exist.

What it does

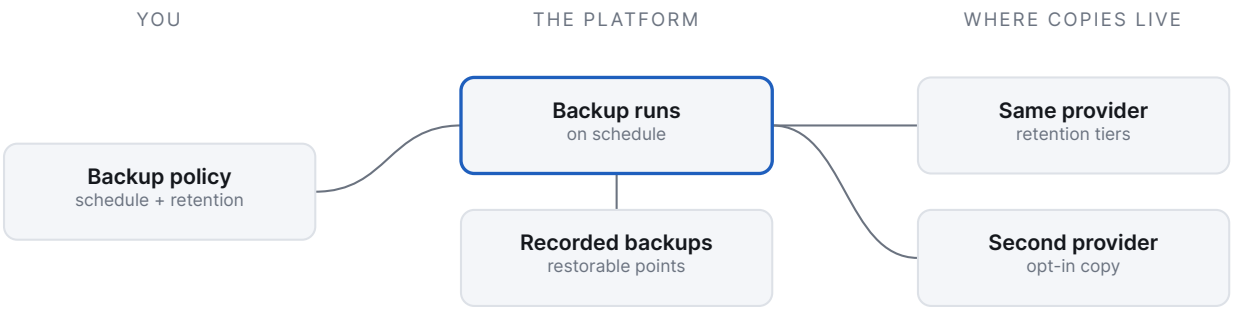
Backup policies
Retention tiers that decide how long each generation is kept, applied as policy rather than a cron a person maintains.

Set the tiers once — how many generations, kept how long — and the platform applies them. There is no script to rot, no job to silently stop running, and every action lands on the audit chain.

Cross-provider copies
A durability flag that copies a backup to a second provider, off by default because it doubles cost and on by an explicit, audited choice.

A backup that lives only where the thing it protects lives is no backup when that place is the outage. One flag puts a copy at a second provider — visibly priced, explicitly chosen, and recorded.

How it fits together



You attach a backup policy to a resource. The platform takes each backup on schedule, keeps generations by retention tier, optionally copies them to a second provider, and every restore names the recorded backup it came from.

Key ideas

Retention tier

How long each generation of backup is kept — daily, weekly, monthly — applied by the platform as policy rather than by a script someone maintains.

Cross-provider copy

An explicit choice to keep a copy with a second provider, so one outage cannot take the original and its backup together. Off by default, because it doubles the cost.

Archive tier

A colder, cheaper place for backups you must keep but rarely read, with a stated retrieval time.

In depth

Policy, not scripts

Schedules and retention are properties of the policy, so there is no cron job to forget and no copy kept forever by accident.

Restores you can name

Every restore comes from a recorded backup, so recovery is a defined operation with a defined source — not a search for whatever copy might exist.

Databases and volumes too

Databases keep continuous backups for point-in-time recovery, and volumes take snapshots on a schedule — the same idea, built into each resource.

How it works

01 **Set a policy** · Console
Retention tiers decide how long each generation of backups is kept — policy, not a cron job someone maintains.

02 **Let the platform apply it** · Policy
Generations are kept and expired by the policy itself, with every action on the audit chain.

03 **Copy to a second home** · Console
An explicit durability flag copies a backup to a second provider, so one outage cannot take both.

04 **Restore when it matters** · API
Restores come from a recorded source, so a wrong timestamp costs a throwaway copy, not the original.

Who it is for

Compliance-driven teams

Retention obligations with evidence the policy was followed.

Retention tiers applied as platform policy, every action on the audit chain.

Disaster recovery planners

A backup that survives the loss of its provider.

Cross-provider copies enabled by one explicit, audited flag.

Operators before a change

A defined way back before upgrades and migrations.

Recorded backups every restore can name as its source.

Works with

Console · API · TypeScript SDK

Questions buyers ask

How long are backups kept?
As long as your retention tiers say. The policy decides how long each generation is kept, and the platform applies it — nothing depends on a person remembering.

Can a backup survive losing a whole provider?
Yes, if you enable the cross-provider durability flag for that backup. It is off by default because it doubles cost, and turning it on is an explicit, audited choice.

How do I know a restore will work?
Every restore names the recorded backup it comes from, so recovery is a defined operation with a known source rather than a search.

How is it billed?
By the gigabyte stored at the published rate, with the cross-provider copy adding its visible cost when you choose it. The rates are on the pricing page.

Pricing

Current published rates, in your currency: https://adaydev.com/pricing/cloud