

USE CASE

Connect cloud accounts read-only and see which failed

Connect AWS, Azure and GCP accounts with read-only access and see which ones Aribot could actually read, so an unread account never passes as clean.

THE PROBLEM

Security tools ask for write access on day one, and that conversation stalls with the cloud team. New accounts get added by different teams, and nobody tracks which ones are being scanned. Our last quarterly report looked clean, and one subscription had never been scanned at all.

HOW ARIBOT HANDLES IT

- 1 Add the first account**
Grant a read-only role, and the account connects without anything in it changing.
- 2 Add the rest**
Connect further AWS, Azure and GCP accounts the same way.
- 3 Read the estate**
Aribot reads the live inventory and brings resources into scope.
- 4 See what failed**
Accounts that could not be read are named, for example one that returned permission denied.

WHAT YOU SEE IN THE DEMO

- Account statuses of CONNECTED, PERMISSION DENIED and NEVER SCANNED
- Counters for accounts added, successfully read and not readable
- An accounts table with last scan, compliance, violations and an enable switch
- Tabs for scan history, standards, remediation and the compliance scanner

WHO IT IS FOR

- Head of Cloud Security
- Cloud Security Architect
- Head of Platform Engineering

WHAT YOU GET

- Findings from read-only access
- A named list of accounts that could not be read
- Resource counts that state they come from readable accounts only
- Scan, compliance and violation status for every account in one table

See it: ayurak.com/demos/cloud-accounts

€30 per scan · €30 per applied fix (dry runs free)