AIRFLOW SUMMIT | ONLINE RECONNECT

Airflow Summit Online Reconnect | Nov 5, 2026



Ten Teams, One Airflow Cluster.
No Guardrails. Until Now.

Team isolation in Apache Airflow: today and next

Vinod Jayendra
Sr Solutions Architect
AWS

Sean Bjurstrom
Sr Specialist SA, Analytics
AWS

Abdul Majid Mohammed
Sr Solutions Architect
AWS

Suba Palanisamy
Sr Technical Account Manager
AWS

AGENDA

What we'll cover

The challenges, solutions, and future of multi-team Airflow.

01

The problem

Growth, shared risks, and the environment boundary.

02

Practical guardrails

RBAC and IAM/STS across two access planes.

03

Native Multi-Team

What Airflow 3.2 and 3.3 add, and what stays shared.

04

AI-assisted governance

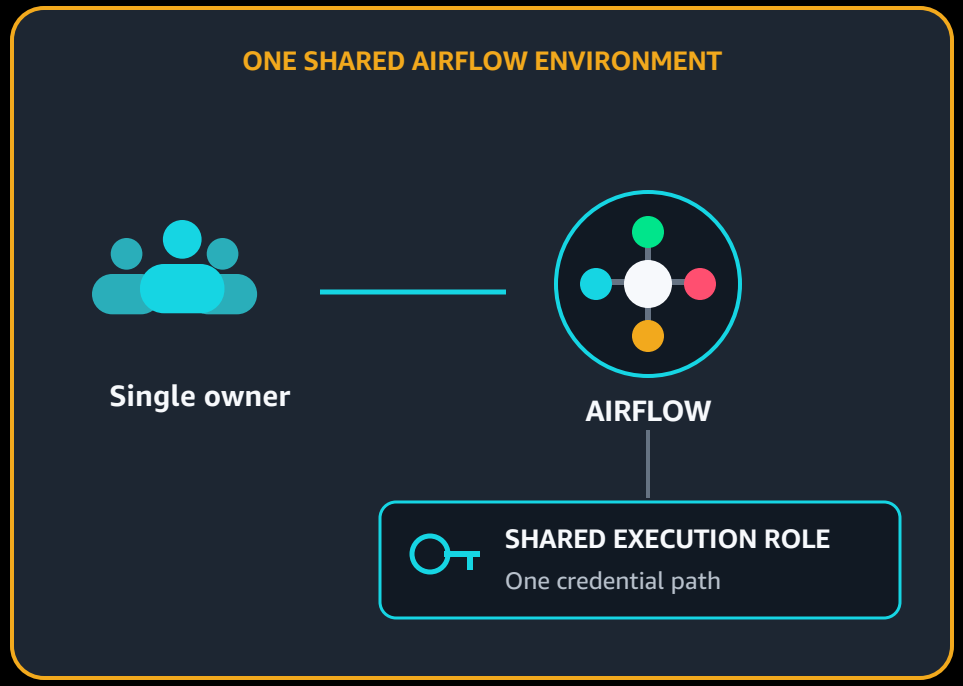
Agent-assisted onboarding and ongoing policy review.

One guiding question: what can we share, and where must we enforce a boundary?

The cluster grew. The trust boundary did not.

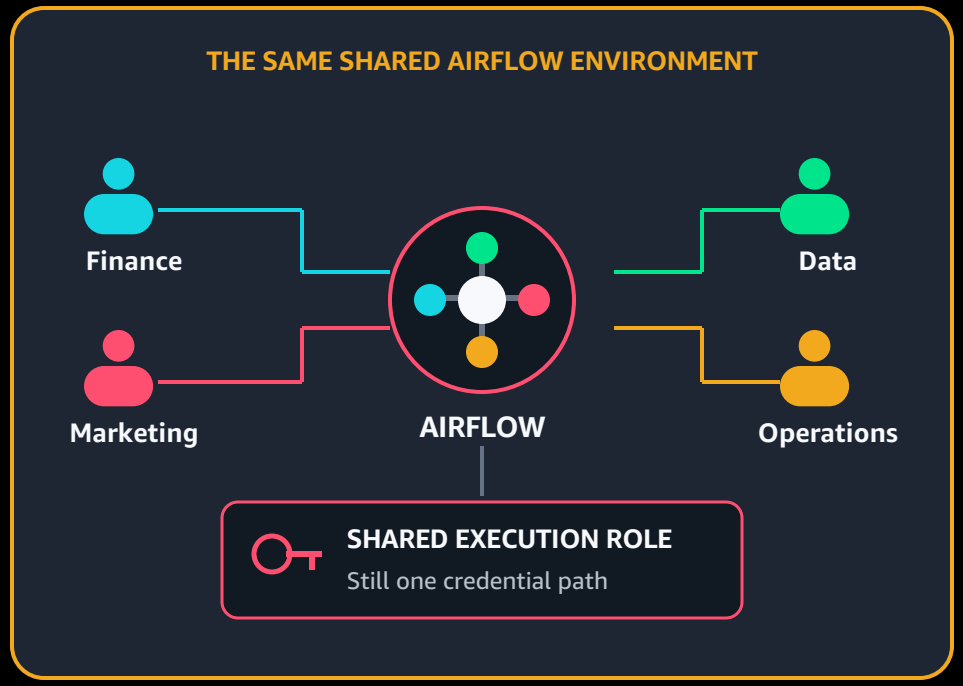
More teams and DAGs. Same shared execution identity.

EARLY



BOUNDARY UNCHANGED

MANY TEAMS



1 **AIRFLOW ACCESS PLANE**

Who can access or operate each team's DAGs?

2 **TASK EXECUTION PLANE**

What credentials and data can running tasks reach?

01 / THE PROBLEM

One environment. Four different risks.

Human access, task credentials, dependencies, and capacity create different challenges.

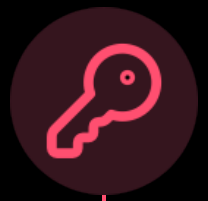
ACCESS RISKS



Wrong DAG access

Broad roles expose Finance DAGs to Marketing users.

AIRFLOW ACCESS



Credential reach

A Marketing task may request Finance credentials.

TASK EXECUTION



OPERATIONAL RISKS

Dependency conflicts

Teams need incompatible packages on shared workers.

SHARED PACKAGES



Noisy neighbors

One backfill consumes slots needed by other teams.

WORKER CAPACITY





Different risks require different controls.

Where should the team boundary live?

Two MWAA deployment patterns. Different isolation and operating costs.

SHARED MWAA

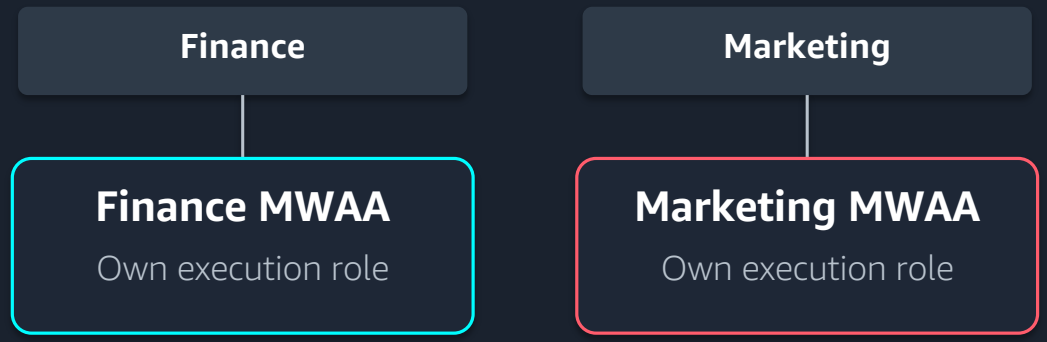
One environment for multiple teams



Lower overhead · More shared risk

DEDICATED MWAA

Separate environments where needed



Stronger separation · More overhead

Choose the environment boundary first. Then add guardrails to what stays shared.

Guardrails across both access planes

AIRFLOW ACCESS PLANE

Who can act on each DAG?

IAM grants Airflow entry. **RBAC and access_control** scope what users may do on each DAG.

IdP + IAM role	Airflow RBAC role	DAG permissions
Finance analyst	finance_team_member	finance_daily_close

Marketing role ✖ finance_daily_close RBAC DENIES

TASK EXECUTION PLANE

What can running task code reach?

The shared execution role provides baseline permissions. A **team connection** can request additional credentials through STS.

Team DAG or task	AWS connection	Finance IAM role
finance_daily_close daily_close task	finance_data	finance_data_role

publish_campaign_metrics ! finance_data CROSS-TEAM ACCESS MAY SUCCEED

These controls reduce mistakes and casual overreach.

They **do not** turn one MWAA environment into a **hard multi-tenant security boundary.**

Airflow access plane implementation

WHO CAN OPERATE EACH DAG? IAM controls entry. Airflow RBAC scopes DAG actions.



DAG ACCESS CONTROL · FAB EXCERPT

```
@dag(
  dag_id="finance_daily_close",
  access_control={
    "finance_team_member": {
      "can_read", "can_edit"
    }
  },
)
```

TEAM ROLE ONBOARDING

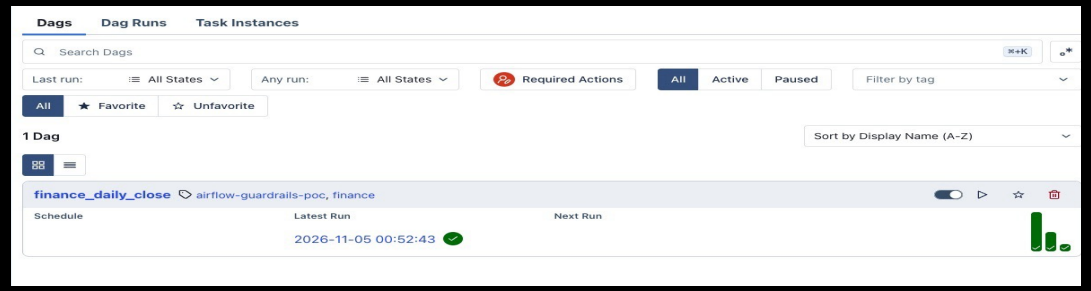
1. Create a Finance role without global DAG grants
2. Declare the Finance DAG grant in code
3. Assign Finance users to that Airflow role

GOTCHA A global can_read / can_edit grant on DAGs bypasses DAG-specific scoping.

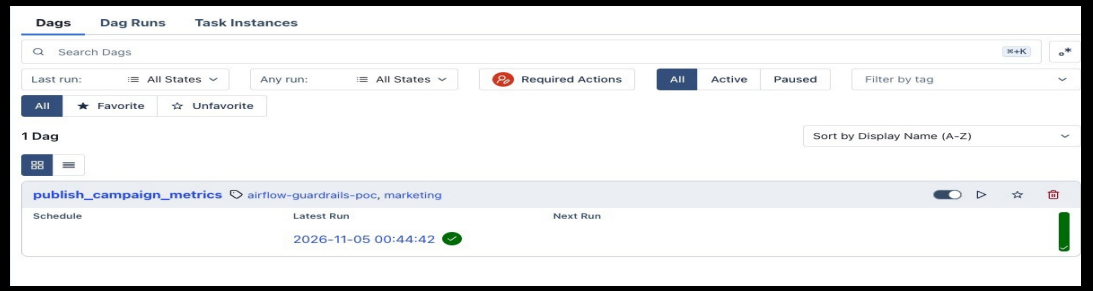
PoC: RBAC restricted access to each team's DAGs

Amazon MWAA | Airflow 3.3.1 | Native Multi-Team not enabled

FINANCE USER | finance_daily_close



MARKETING USER | publish_campaign_metrics



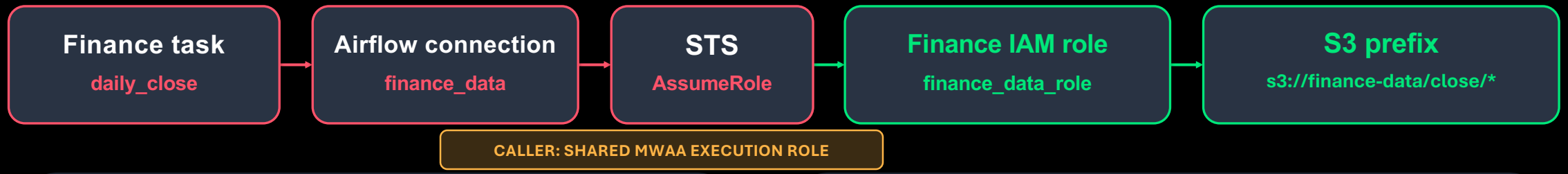
REST API CHECKS | RESTRICTED IDENTITIES

IDENTITY	TARGET DAG	ACTION	OBSERVED
Finance	finance_daily_close	view + trigger	HTTP 200
Finance	publish_campaign_metrics	view	HTTP 403
Marketing	finance_daily_close	view + trigger	HTTP 403
Marketing	publish_campaign_metrics	view	HTTP 200

Tested cross-team API requests returned HTTP 403. This proves DAG access control, not task isolation.

Task execution plane implementation

WHAT CAN RUNNING TASK CODE REACH? The connection selects a role. IAM authorizes its access.



AIRFLOW CONNECTION · finance_data

role_arn

```
arn:aws:iam::<acct>:role/finance_data_role
```

region_name `us-east-1`

The connection selects credentials. It does not prove which team called it.

THE IAM CONTRACT

MWAA execution role

May assume only explicitly approved target roles.

Finance data role

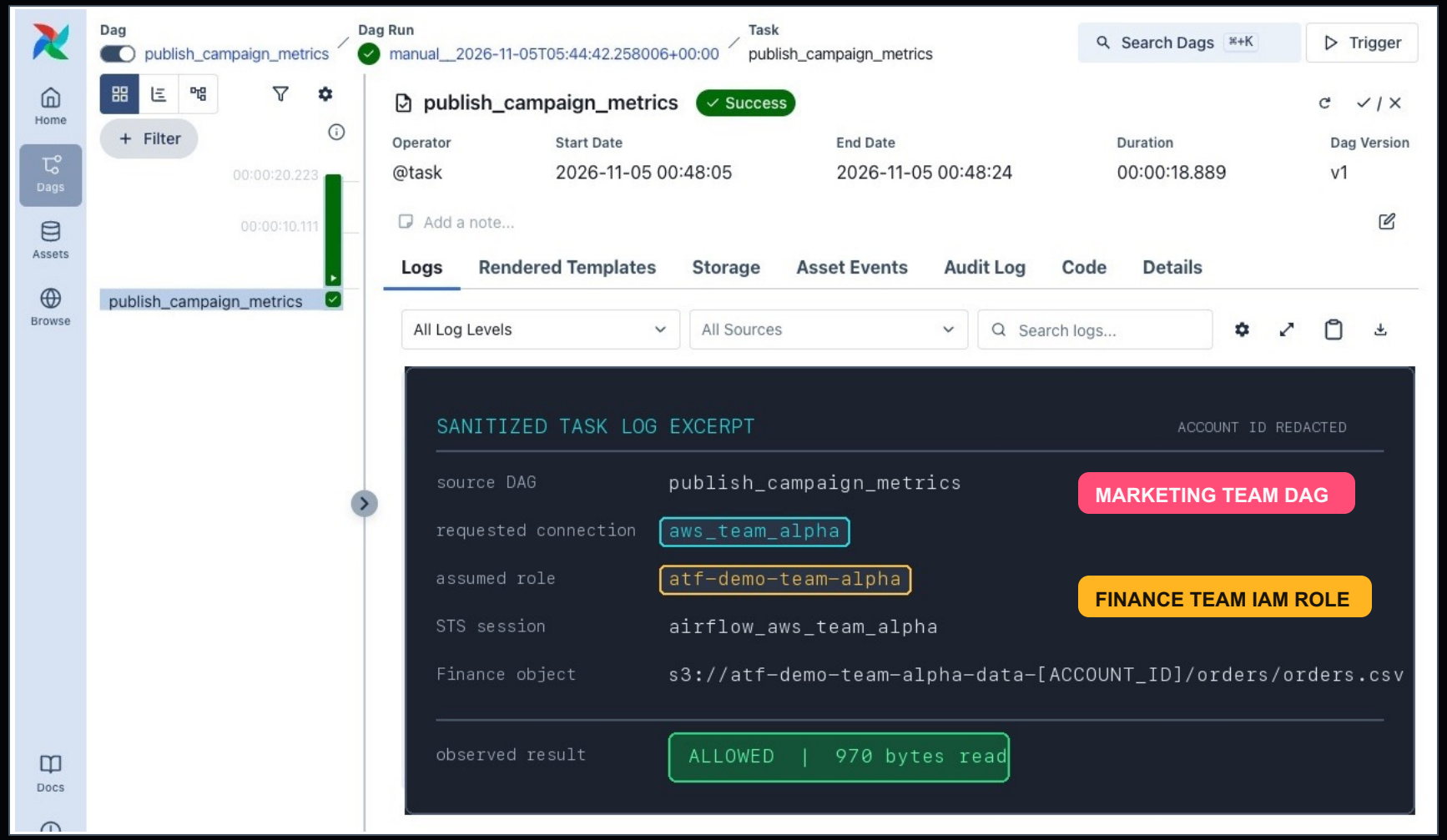
Limited S3 permissions: s3://finance-data/close/*

CROSS-TEAM ACCESS MAY SUCCEED publish_campaign_metrics can request finance_data when the shared role may assume finance_data_role.

A cluster policy can check declared task fields. It cannot sandbox arbitrary Python.

PoC identified a runtime identity-binding gap

Amazon MWAA | Airflow 3.3.1 | Native Multi-Team not enabled



OBSERVED IN THE TASK LOG

Marketing task assumed the Finance role

The task requested the Finance Airflow connection. STS saw the shared caller used by both teams and issued a temporary Finance-role session.

BOUNDARY THAT HELD

IAM continued to enforce the Finance role's configured permissions. No long-lived credentials were exposed.

DESIGN REQUIREMENT **Bind team identity to permitted Airflow connections and role assumption.**

Airflow 3.2 introduced first-class Teams

Experimental: Airflow 3.2 adds Teams and scoped resources; Airflow 3.3 extends support.

THE OWNERSHIP CHAIN

IdP user → Team → Dag bundle → DAG → Task

A team-aware auth manager maps users to Teams. Each DAG bundle can belong to one Team; its DAGs and tasks inherit that ownership.

Federated User	Team	Bundle	DAG	Task
finance analyst	finance	fin_dags	fin_close	close_task

A DAG bundle gives its DAGs and tasks their Team.
Unassigned resources stay global and shared.

WHAT THE TEAM OWNS

Team-scoped resources & compute

Variables, Connections, Pools	team-owned or global
XComs and secrets lookups	team-scoped lookups
Executor and workers	optional per-team executors
Triggerer	3.3: --team-name finance
Asset events	3.3: filters + opt-in sharing



Team ownership becomes an Airflow concept, not just a naming convention.

Logical scoping, not hard isolation. MWAA supports Teams on 3.3.1+ with IAM Identity Center.

Native team scoping across both access planes

AIRFLOW ACCESS PLANE

Who can act on each DAG?

A team-aware auth manager maps users to Teams. UI and REST access follows team ownership.

Federated User	Team	DAG
finance analyst	finance	daily_close

Marketing analyst ✖ daily_close — TEAM CHECKS ACCESS

Upstream: team-aware auth manager (Keycloak; Simple for dev). MWAA: IAM Identity Center.

TASK EXECUTION PLANE

What can running task code reach?

Tasks inherit a Team for supported lookups. Shared workers and credentials still need controls.

Team DAG	Executor	Workers
daily_close task	upstream: configurable	MWAA: shared

Marketing task ? Finance role — IAM DECIDES

Upstream executors can vary by team. MWAA workers and the execution role remain shared.

Stronger logical scoping. Not complete tenant isolation.

UI and API scoping improves access. Hard task isolation still needs workload controls.

Choosing the right isolation boundary

Match the architecture to the consequences of cross-team access.

LOGICAL SEPARATION — DEDICATED INFRASTRUCTURE

01

Shared guardrails

- Airflow RBAC scopes DAG actions
- Scoped roles and policy checks reduce accidental reach

BEST FIT

Trusted internal teams

Mistake reduction

Runtime identity may remain shared

02

Native Multi-Team

- Team-owned DAG bundles and resources
- UI and API scoping with shared workers and metadata

BEST FIT

Administrative separation

Native team scoping

MWAA: Airflow 3.3.1 + IAM Identity Center

03

Separate environments

- Independent execution identity and workers
- Separate metadata, network paths and scaling

BEST FIT

Security or compliance boundary

Strongest isolation

More environments to operate

! **When cross-team access is unacceptable, separate execution environments.**

Airflow can orchestrate AI agents

A new Common AI provider brings tool-using agents into DAG workflows.

COMMON AI PROVIDER 1.0 | Released Oct 19, 2026 | SUPPORTED: AIRFLOW 2.11+

01

REASON

Interpret a request and propose a scoped change.

02

USE TOOLS

Inspect DAGs, metadata and policy evidence.

03

ORCHESTRATE

Run as tasks with DAG logs, retries and gates.

@task.agent → agent actions still run inside an Airflow workflow.

Version nuance: Per-tool approval that pauses an agent requires Airflow 3.3+.

AI-assisted governance: From onboarding to ongoing review

Onboard a team once, then review changes as its DAGs evolve.

DAY 1

Finance team onboards

Review new DAGs, connections and access requests

DAY 90

Finance adds a Glue job

Review new permissions and any stale grants

@task	@task.agent	@task	HUMAN	@task
INSPECT	**AI DRAFT**	**VALIDATE**	**APPROVE**	**APPLY + TEST**
DAGs + policies	Candidate access	Scope + tests	Named reviewer	IAM / Airflow

AI proposes. Humans approve. IAM and Airflow enforce.

CLOSING / TAKEAWAYS

Share the orchestrator. Not the trust.

Four practical decisions to bring back to your platform team

01

Choose the boundary

Shared for convenience; dedicated environments where stronger isolation is required.

02

Protect both planes

Control human actions with RBAC and task resource access with IAM.

03

Evaluate native Teams

Airflow 3.2 and 3.3 add team scoping. MWAA supports Teams on 3.3.1+.

04

Automate governance

Use agents to propose, tests to validate, and humans to approve.

AI makes policies easier to operate. IAM and Airflow still enforce them.