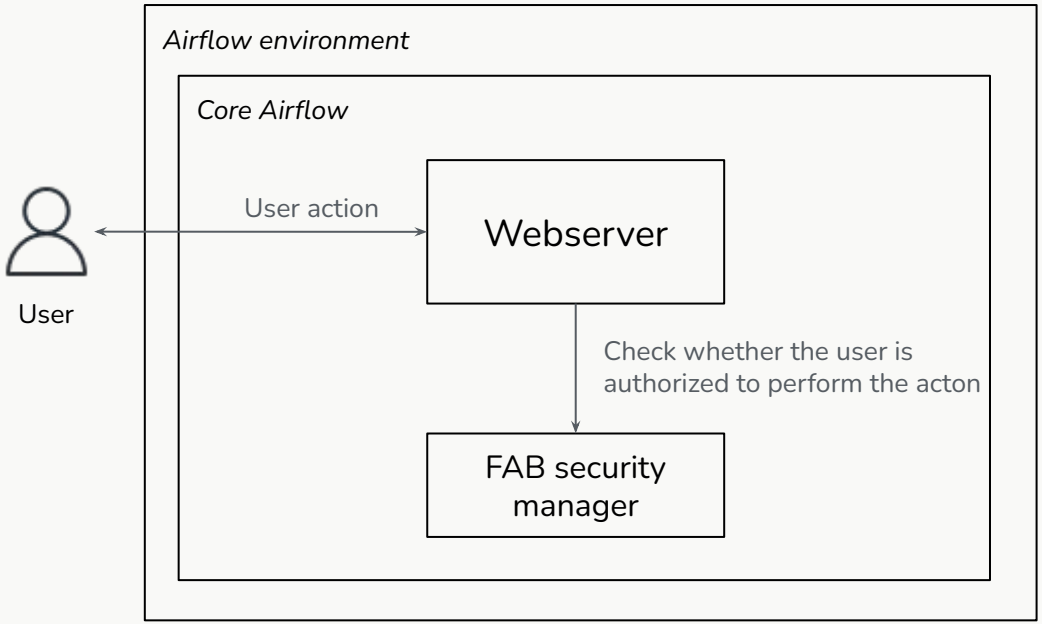
Simplified user management in Airflow

Vincent Beck
Sr software engineer at AWS
Apache Airflow committer

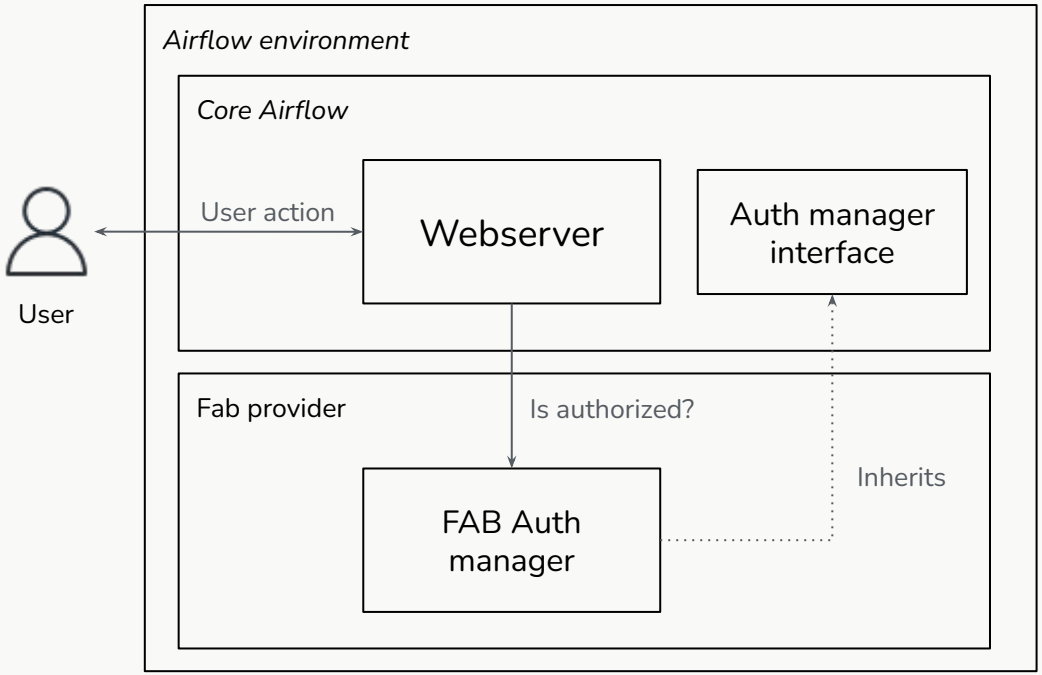
Context

Before Airflow 2.9 and introduction of extensible user management (AIP-56)



Context

Since Airflow 2.9 and introduction of extensible user management (AIP-56)

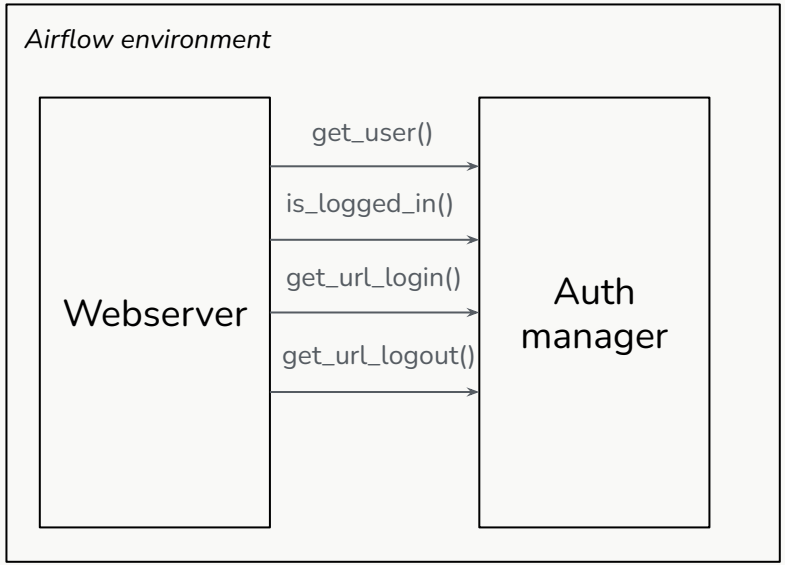


What is an auth manager?

What is the auth manager?

Interface responsible for:

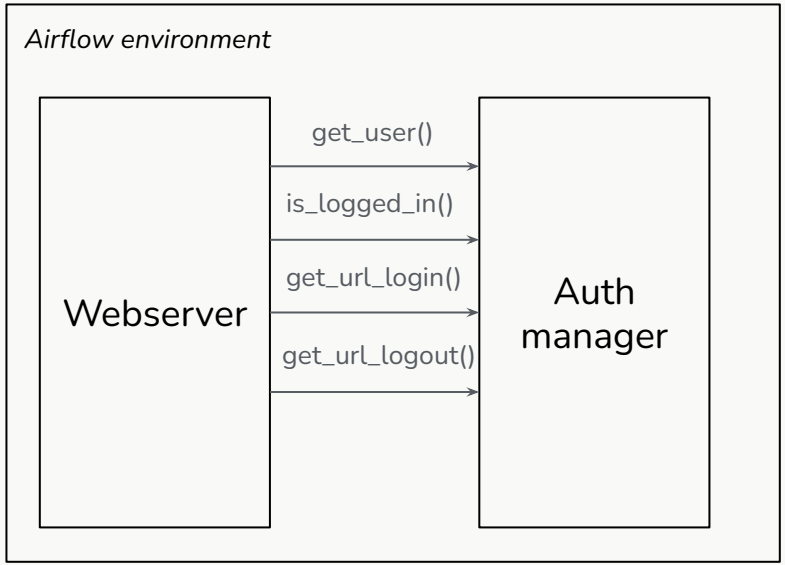
User authentication



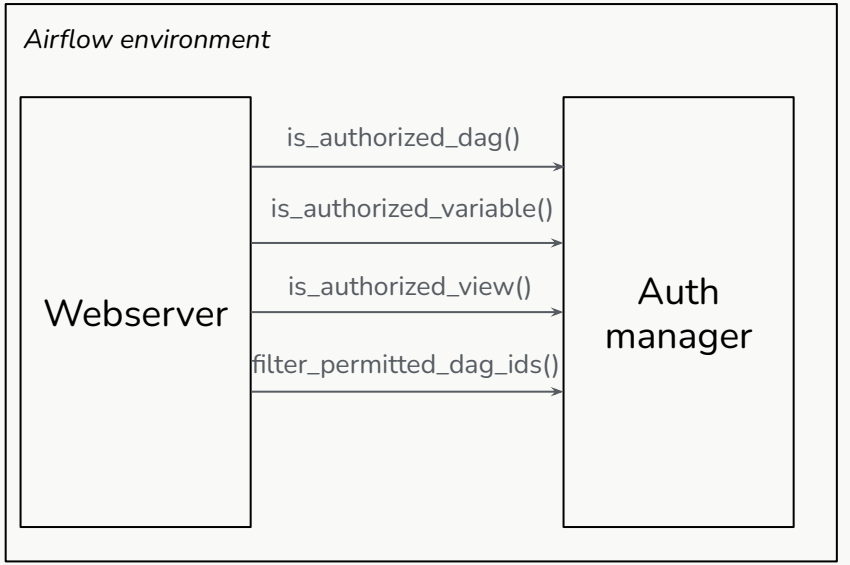
What is the auth manager?

Interface responsible for:

User authentication

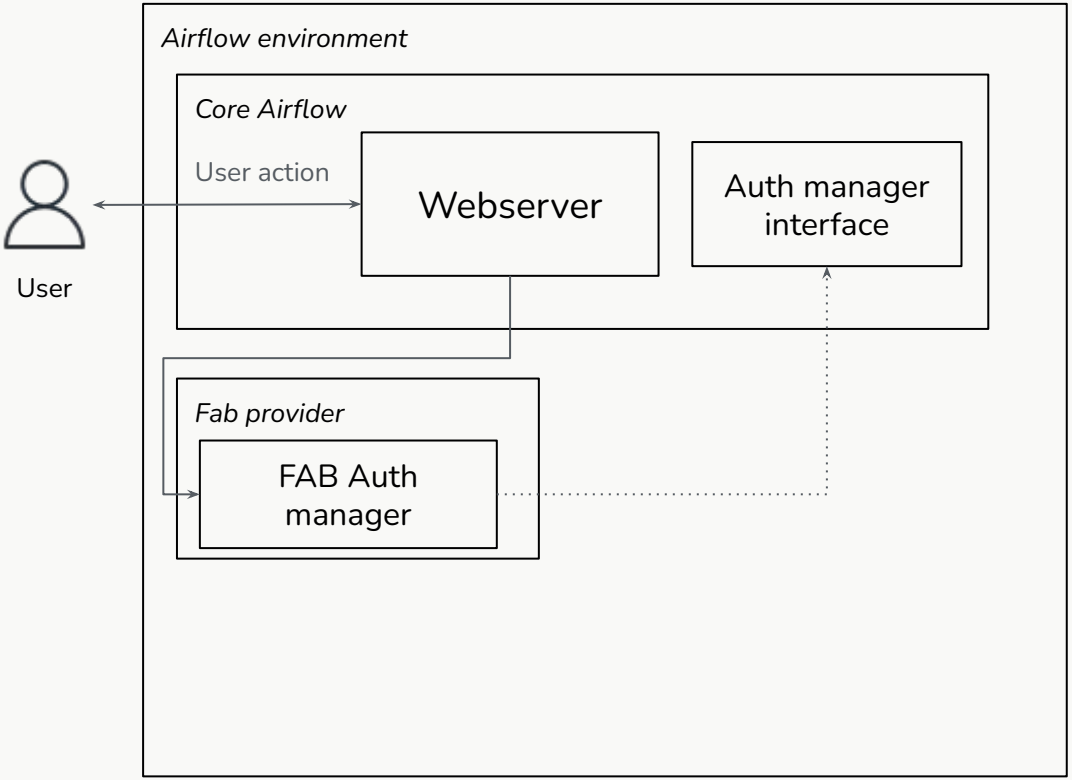


User authorization

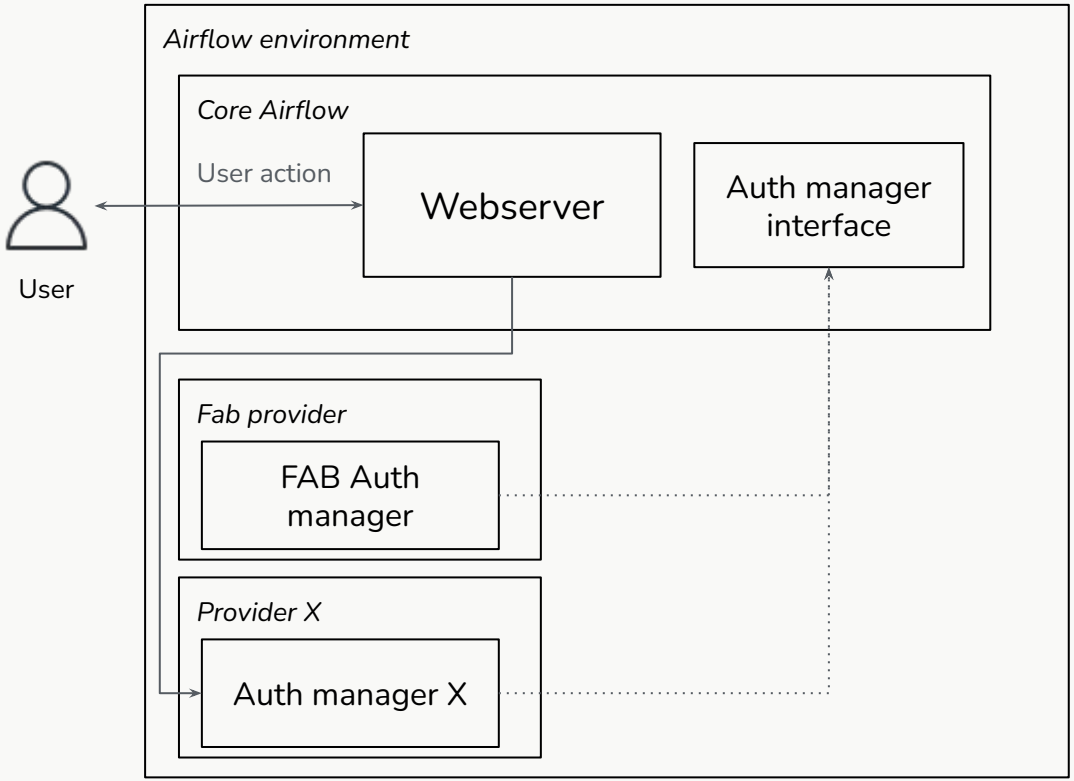


Why an auth manager?

Why an auth manager?

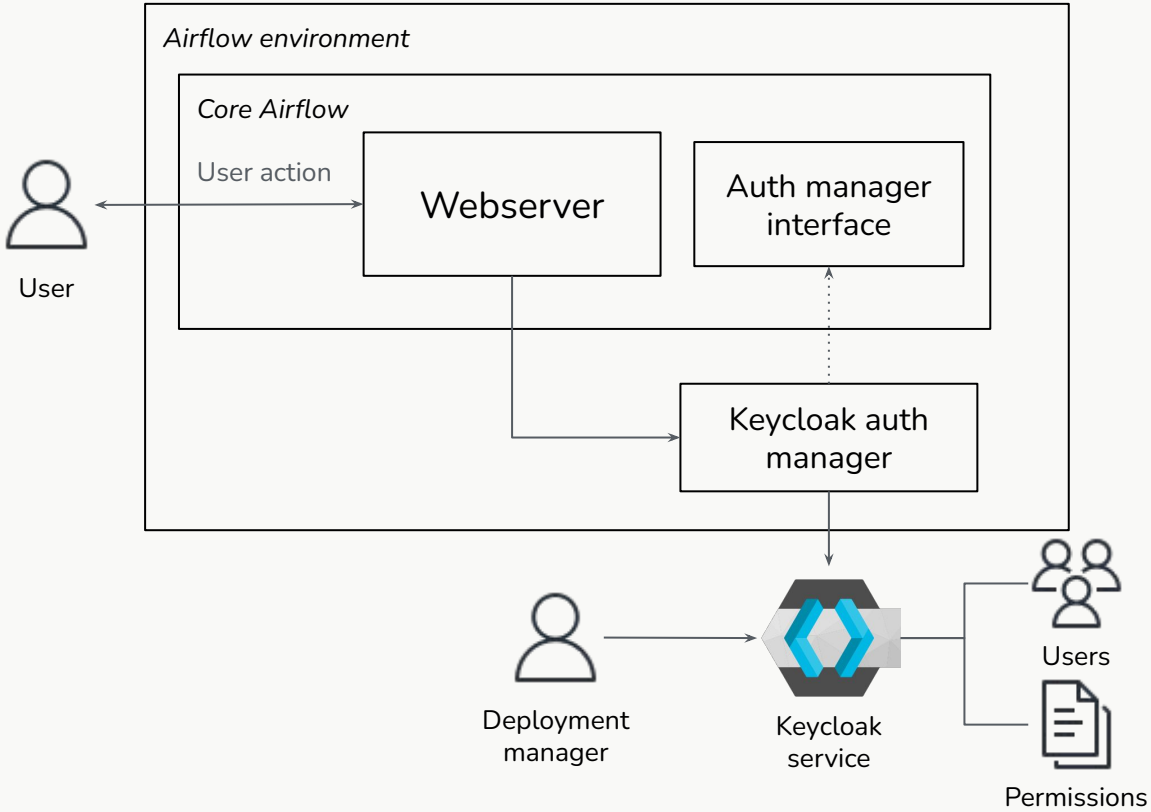


Why an auth manager?




```
[core]
auth_manager =
airflow.providers.X.auth_manager
.XAuthManager
```

Why an auth manager?

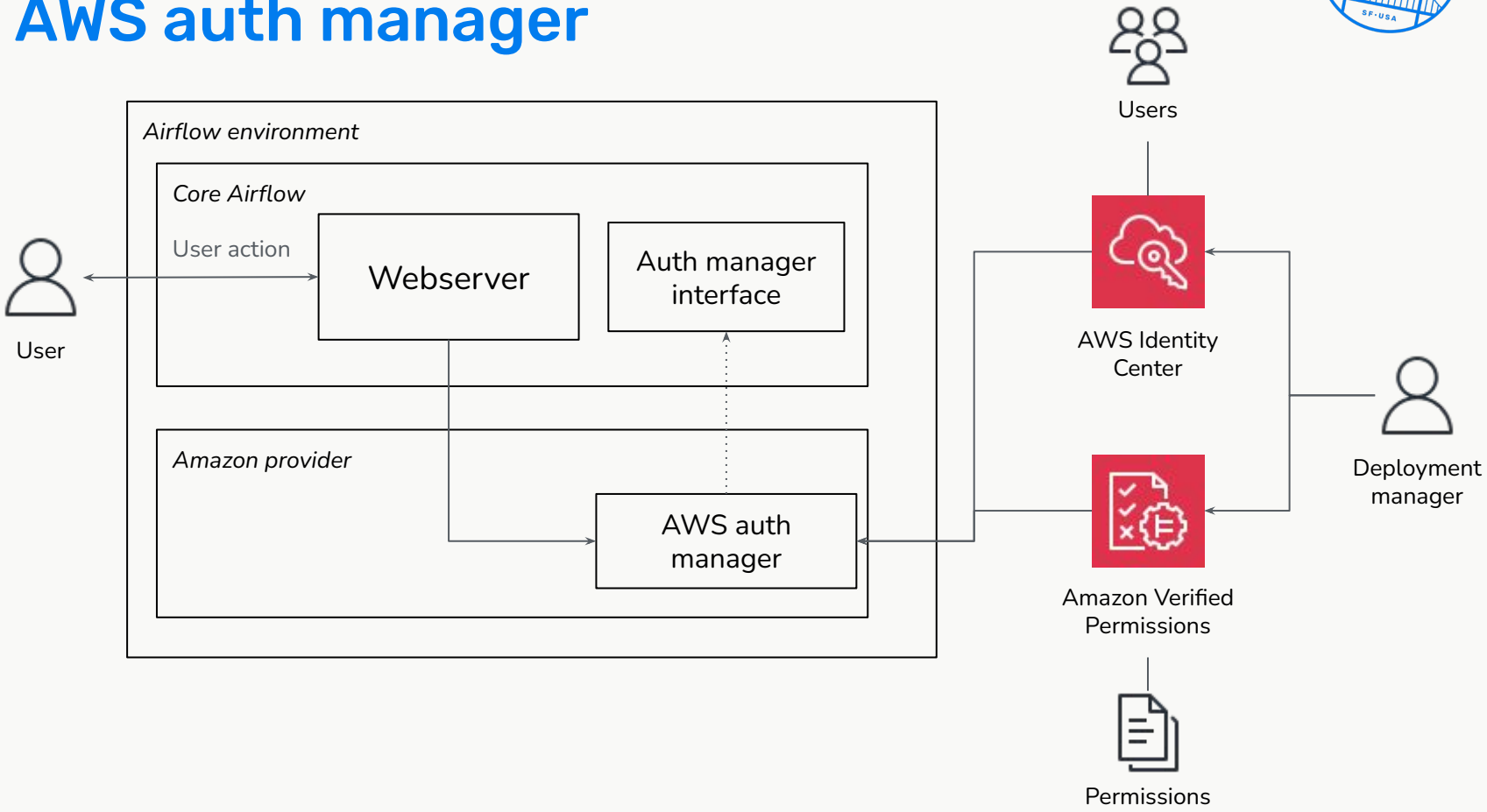


Why an auth manager?

× can read on DAGs × can edit on DAGs × can delete on DAGs × can read on DAG Dependencies × can read on DAG Code × can read on DAG Runs × can read on Datasets ×
× can read on Cluster Activity × can read on Pools × can read on ImportError × can read on DAG Warnings × can read on Jobs × can read on My Password × can edit on My Password
× can read on My Profile × can edit on My Profile × can read on SLA Misses × can read on Task Instances × can read on Task Logs × can read on XComs × can read on Website
× menu access on Browse × menu access on DAGs × menu access on DAG Dependencies × menu access on DAG Runs × menu access on Datasets × menu access on Cluster Activity
× menu access on Documentation × menu access on Docs × menu access on Jobs × menu access on SLA Misses × menu access on Task Instances × can create on Task Instances
× can edit on Task Instances × can delete on Task Instances × can create on DAG Runs × can edit on DAG Runs × can delete on DAG Runs × can create on Datasets × can read on Configurations
× menu access on Admin × menu access on Configurations × menu access on Connections × menu access on Pools × menu access on Plugins × menu access on Variables
× menu access on Providers × menu access on XComs × can create on Connections × can read on Connections × can edit on Connections × can delete on Connections × can create on Pools
× can edit on Pools × can delete on Pools × can read on Plugins × can read on Providers × can create on Variables × can read on Variables × can edit on Variables × can delete on Variables
× can delete on XComs × can delete on Datasets × can read on Audit Logs × menu access on Audit Logs × can read on Task Reschedules × menu access on Task Reschedules × can read on Triggers
× menu access on Triggers × can read on Passwords × can edit on Passwords × can read on Roles × can edit on Roles × can delete on SLA Misses × can edit on SLA Misses × can create on Users
× can read on Users × can edit on Users × can delete on Users × menu access on List Users × menu access on Security × can create on Roles × can delete on Roles × menu access on List Roles
× can read on User Stats Chart × menu access on User's Statistics × can read on Permissions × menu access on Actions × can read on View Menus × menu access on Resources
× can read on Permission Views × menu access on Permission Pairs

AWS auth manager

AWS auth manager




Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon Aug 12 3:07 PM
New Incognito Tab
Incognito
Team
Tools
Interviews
Accounts
Perso
dev@airflow.apac...
All Bookmarks
You've gone Incognito
Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more
Chrome won't save:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider
Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

AWS auth manager

Authorization

- Amazon Verified Permissions
- Uses Cedar language: language to define permissions

AWS auth manager

Give all permissions to a group of users

```
permit (
    principal in Airflow::Group::"Admin",
    action,
    resource
);
```

AWS auth manager

Give all permissions to a group of users

```
permit (
    principal in Airflow::Group::"Admin",
    action,
    resource
);
```

Give DAG specific permissions to a group of users

```
permit (
    principal in Airflow::Group::"Marketing",
    action,
    resource == Airflow::Dag::"marketing"
);
```

AWS auth manager

Give all permissions to a group of users

```
permit (
    principal in Airflow::Group::"Admin",
    action,
    resource
);
```

Give read-only permissions to a group of users

```
permit (
    principal in Airflow::Group::"Viewer",
    action in
        [Airflow::Action::"Connection.GET",
         Airflow::Action::"Dag.GET",
         Airflow::Action::"Pool.GET",
         Airflow::Action::"Variable.GET",
         Airflow::Action::"Dataset.GET",
         Airflow::Action::"View.GET"],
    resource
);
```

Give DAG specific permissions to a group of users

```
permit (
    principal in Airflow::Group::"Marketing",
    action,
    resource == Airflow::Dag::"marketing"
);
```

AWS auth manager

Give all permissions to a group of users

```
permit (
    principal in Airflow::Group::"Admin",
    action,
    resource
);
```

Give read-only permissions to a group of users

```
permit (
    principal in Airflow::Group::"Viewer",
    action in
        [Airflow::Action::"Connection.GET",
         Airflow::Action::"Dag.GET",
         Airflow::Action::"Pool.GET",
         Airflow::Action::"Variable.GET",
         Airflow::Action::"Dataset.GET",
         Airflow::Action::"View.GET"],
    resource
);
```

Give DAG specific permissions to a group of users

```
permit (
    principal in Airflow::Group::"Marketing",
    action,
    resource == Airflow::Dag::"marketing"
);
```

Forbid specific action to specific user

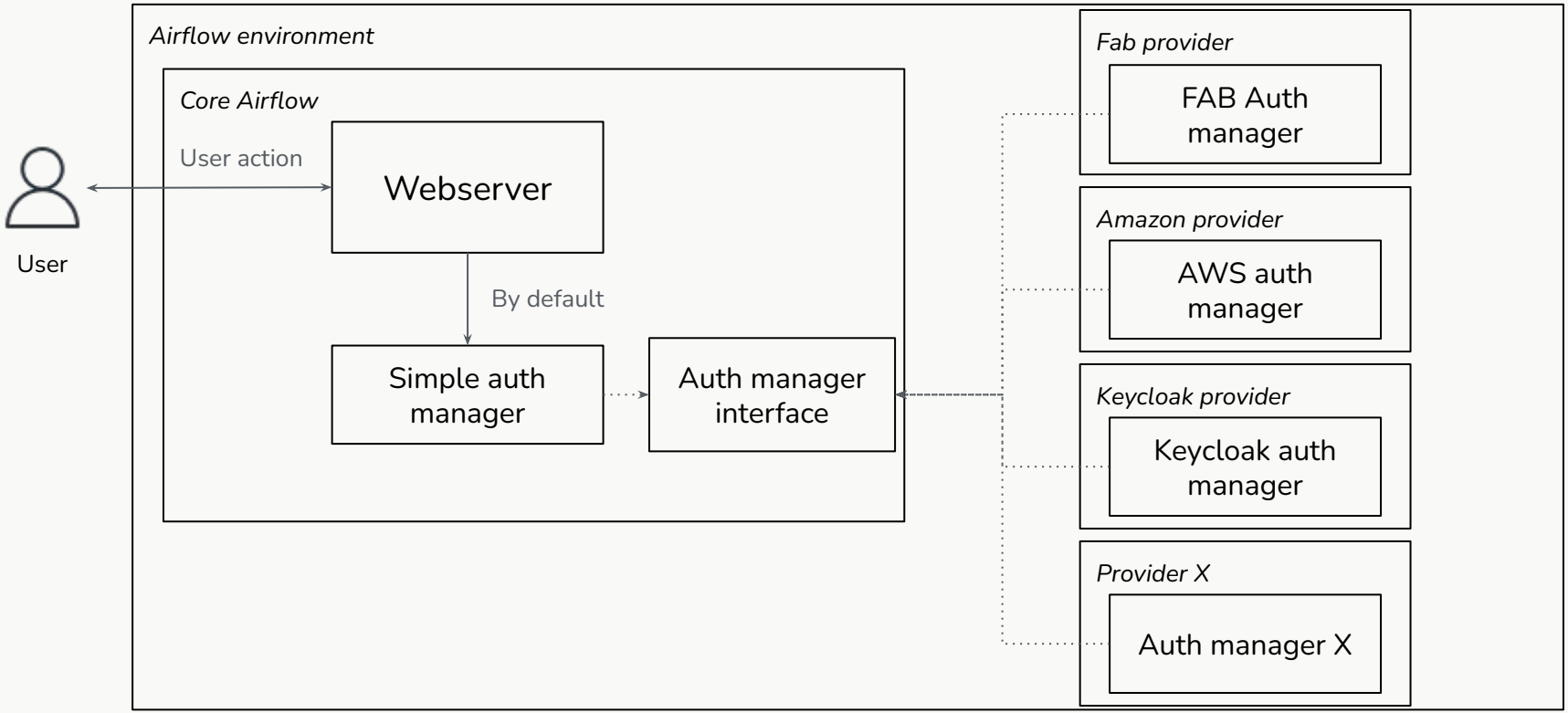
```
forbid (
    principal == Airflow::User::"<id>",
    action,
    resource == Airflow::Dag::"secret-dag-1"
);
```

AWS auth manager - future

```
permit (
    principal in Airflow::Team::"Marketing",
    action,
    resource is Airflow::Dag in Airflow::DagFolder::"marketing"
);
```

Airflow 3 and beyond

Airflow 3 and beyond






Questions?

https://github.com/vincbeck
https://www.linkedin.com/in/vincentbeck