



Science and
Technology
Facilities Council

The IRIS Accounting Dashboard and IAM

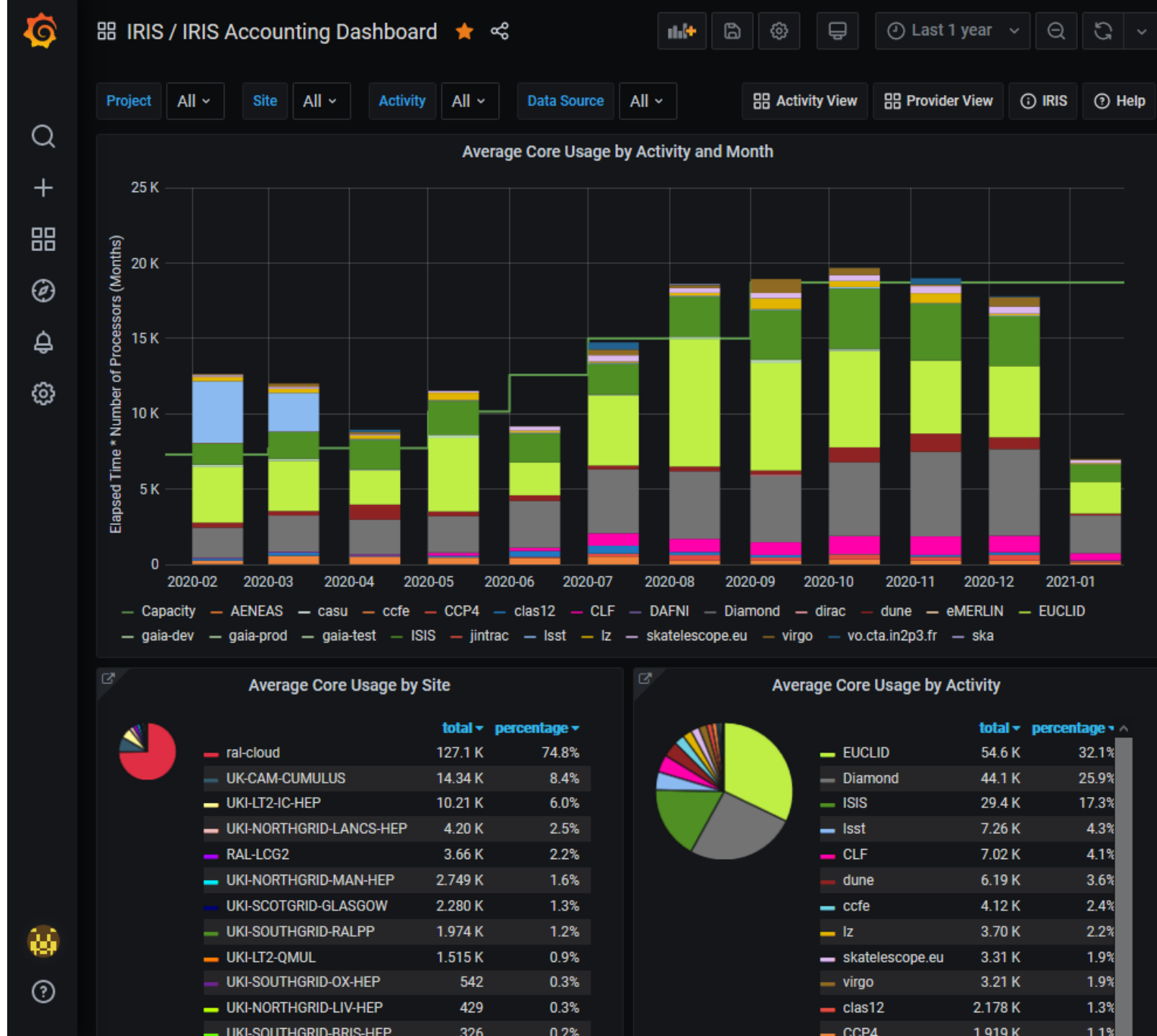
Adrian Coveney
IAM Users Workshop
28th January 2021

Outline

1. The IRIS Accounting Dashboard
2. Why IAM?
3. Registering a Grafana client
4. Illustrated steps
5. Results
6. Future
7. Help

The IRIS Accounting Dashboard

- Dedicated IRIS Accounting Repository using MariaDB based on the APEL Repository schemas and software
- Bespoke Grafana dashboard to explore the data



Why IAM?

- Before IAM
 - To avoid user management, there was a single shared user account and a single shared admin account (data not particularly sensitive at the moment)
- After IAM
 - Accounts automatically created on first login via IRIS IAM
 - Can see who's actually using the Dashboard
 - Possibility for future authorisation controls via IAM groups (though limitations, see later)

Registering a Grafana client

1. Sign in to IAM portal with institute ID
2. Wait for account to be approved
3. Register a new client in IAM portal
4. Update Grafana configuration
5. Try it out
6. Tweak client settings in IAM portal (mainly redirect URLs and scopes)
7. Goto 4

Illustrated steps



Welcome to IRIS IAM

Sign in with your IRIS IAM credentials

A text input field for the username, with a person icon on the left and a clear button on the right.A password input field, with a lock icon on the left and a clear button on the right.

Sign in

[Forgot your password?](#)

Or sign in with

Your Organisation via eduGAIN

[Not a member?](#)

Apply for an account

[About Us, Contact information and Privacy Policy](#)



PERSONAL

Manage Approved Sites

Manage Active Tokens

View Profile Information

DEVELOPER

Self-service client registration

Self-service protected resource registration

Register a new client

Use this form to register a new client with the authorization server. You will be given a client ID and a registration access token to manage your client.

+ New Client

Edit an existing client

Use this form to edit a previously-registered client. Paste in your client ID and registration access token to access the client.

Enter Client ID

Enter Registration Access Token

Edit Client

PERSONAL

- Manage Approved Sites
- Manage Active Tokens
- View Profile Information

DEVELOPER

- Self-service client registration
- Self-service protected resource registration

Home / Self-service Client Registration / Edit an existing client

Edit Client

Save

Cancel

Delete

- Main
- Access
- Credentials
- Crypto
- Other
- JSON

Warning! You MUST protect your **Client ID**, **Client Secret (if provided)**, and your **Registration Access Token**. If you lose your Client ID or Registration Access Token, you will no longer have access to your client's registration records and you will need to register a new client.

Client name

Human-readable application name

Redirect URI(s)

-
-
-

URIs that the client can be redirected to after the authorization page

PERSONAL

- Manage Approved Sites
- Manage Active Tokens
- View Profile Information

DEVELOPER

- Self-service client registration
- Self-service protected resource registration

Edit Client

Save

Cancel

Delete

Main

Access

Credentials

Crypto

Other

JSON

Scope

new scope	<input type="checkbox"/>
openid	<input checked="" type="checkbox"/>
profile	<input checked="" type="checkbox"/>
email	<input checked="" type="checkbox"/>
address	<input type="checkbox"/>
phone	<input type="checkbox"/>
offline_access	<input type="checkbox"/>
preferred_username	<input type="checkbox"/>
eduperson_scoped_affiliation	<input type="checkbox"/>
eduperson_entitlement	<input type="checkbox"/>

OAuth scopes this client is allowed to request

/etc/grafana/grafana.ini

```
[auth.generic_oauth]
enabled = true
name = IRIS IAM
allow_sign_up = true
client_id = *****
client_secret = *****
scopes = openid email profile
auth_url = https://iris-iam.stfc.ac.uk/authorize
token_url = https://iris-iam.stfc.ac.uk/token
api_url = https://iris-iam.stfc.ac.uk/userinfo
allowed_domains = ... stfc.ac.uk ...
```

Results



Welcome to Grafana

Built better together

Email or username

Password

Log in

[Forgot your password?](#)

or



Sign in with IRIS IAM



Configuration

Organization: IRIS

Data Sources

Users

Teams

Plugins

Preferences

API Keys

Search user by login, email or name

Invite

Login	Email	Name	Seen	Role			
			8M	Viewer			
			1M	Viewer			
			10M	Viewer			
	adrian.coveney@stfc.ac.uk	adrian.coveney@stfc.ac.uk	Adrian Coveney	< 1m	Admin		
			3M	Viewer			
			6d	Viewer			
			16d	Viewer			
			3M	Viewer			
			1M	Viewer			
			2d	Viewer			
			1d	Viewer			
	apel_admin	apel_admin@localhost		3M	Admin		

Future

- Open Source version of Grafana allows role mapping from OAuth to the limited set of Grafana roles (i.e. Viewer, Editor or Admin). May be useful if we want to hide some things from general users.
- Enterprise version of Grafana has “Team Sync”, though not clear if it can be used with generic OAuth.

Help

- <https://grafana.com/docs/grafana/latest/auth/generic-oauth/>
- IRIS IAM team
- apel-admins@stfc.ac.uk



Science and
Technology
Facilities Council

Thank you