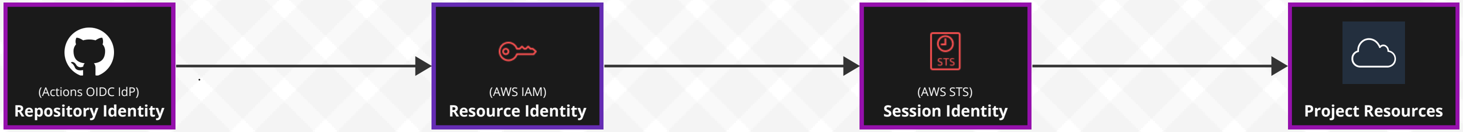
Utopia: Directly enforce resource naming in IAM based on OIDC claims

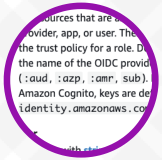


```
n_number": "10",
"run_attempt": "2",
"actor": "octocat",
"workflow": "example-wo
"head_ref": "",
"base_ref": "",
"event_name": "workflow
"ref_type": "branch",
"job_workflow_ref": "
": "https://t
```

GitHub Docs
How the token works with reusable workflows

🔐 - cryptographically signed

- includes details for the calling action & its repo



sources that are a
provider, app, or user. The
the trust policy for a role. D
the name of the OIDC provid
(`:aud`, `:azp`, `:amr`, `sub`).
Amazon Cognito, keys are de
`identity.amazonaws.co`

with stri

AWS Docs
Available keys for AWS web identity federation

can only access OIDC claims for:
- :aud
- :azp
- :amr
- :sub

🚫 can't access repo information as a templated variable due to custom claims :(

```
1566583354,
n_time": 156658329
ttps://aws.amazon.com/t
  "principal_tags": {
      "Project": ["Autom
      "CostCenter": ["987
      "Department": ["En
  },
  "transitive_tag_keys
      "Project",
```

AWS Docs
Passing session tags using AssumeRoleWithWebIdentity

The Actions OIDC IdP isn't capable of writing repo information
in AWS' custom session tags format,
it can only change the format for
`sub` claims

💥 we still can't access the repo information as a templated variable since GitHub can't emit AWS' session tag format :(

■ **Externally Managed Resource**
with load-bearing security responsibilities