Databend

Databend Cloud 云上 IaC 实践

彭川

Databend

Content

01 为什么我们需要 IaC

02 如何使用 IaC

03 Databend Cloud 在使用过程中遇到的问题

Databend

Part 1

为什么我们需要 IaC

多云环境

多集群需求

EKS

Amazon
Elastic Kubernetes Service

AKS

Azure
Kubernetes Service

GKE

Google
Kubernetes Engine

部署方式的易用性和稳定性

- Reproducible
- Declarative
- Reliable

Part 2

如何使用 IaC

Databend

GitOps

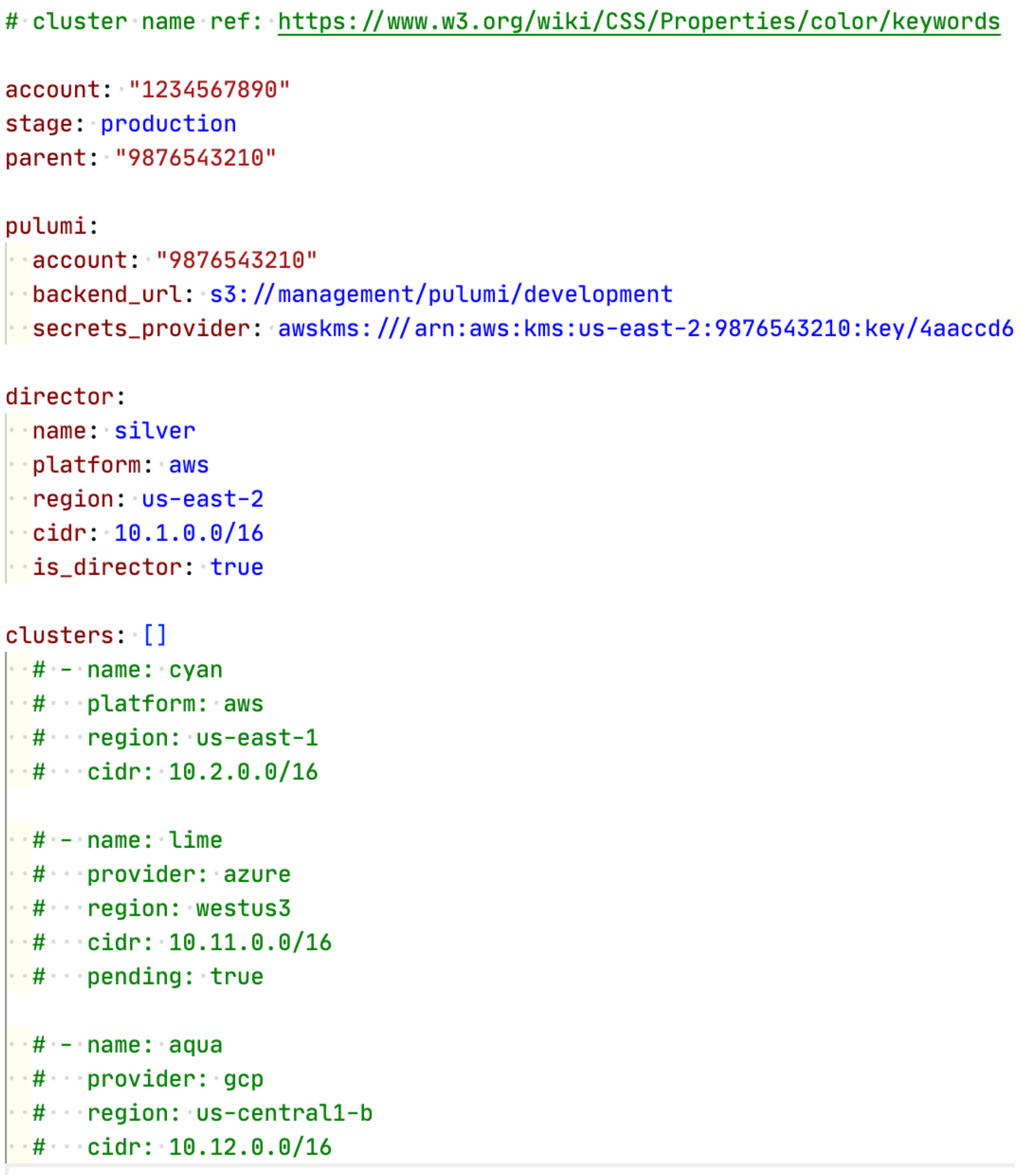
- Terraform
- Pulumi
- Helm

Databend

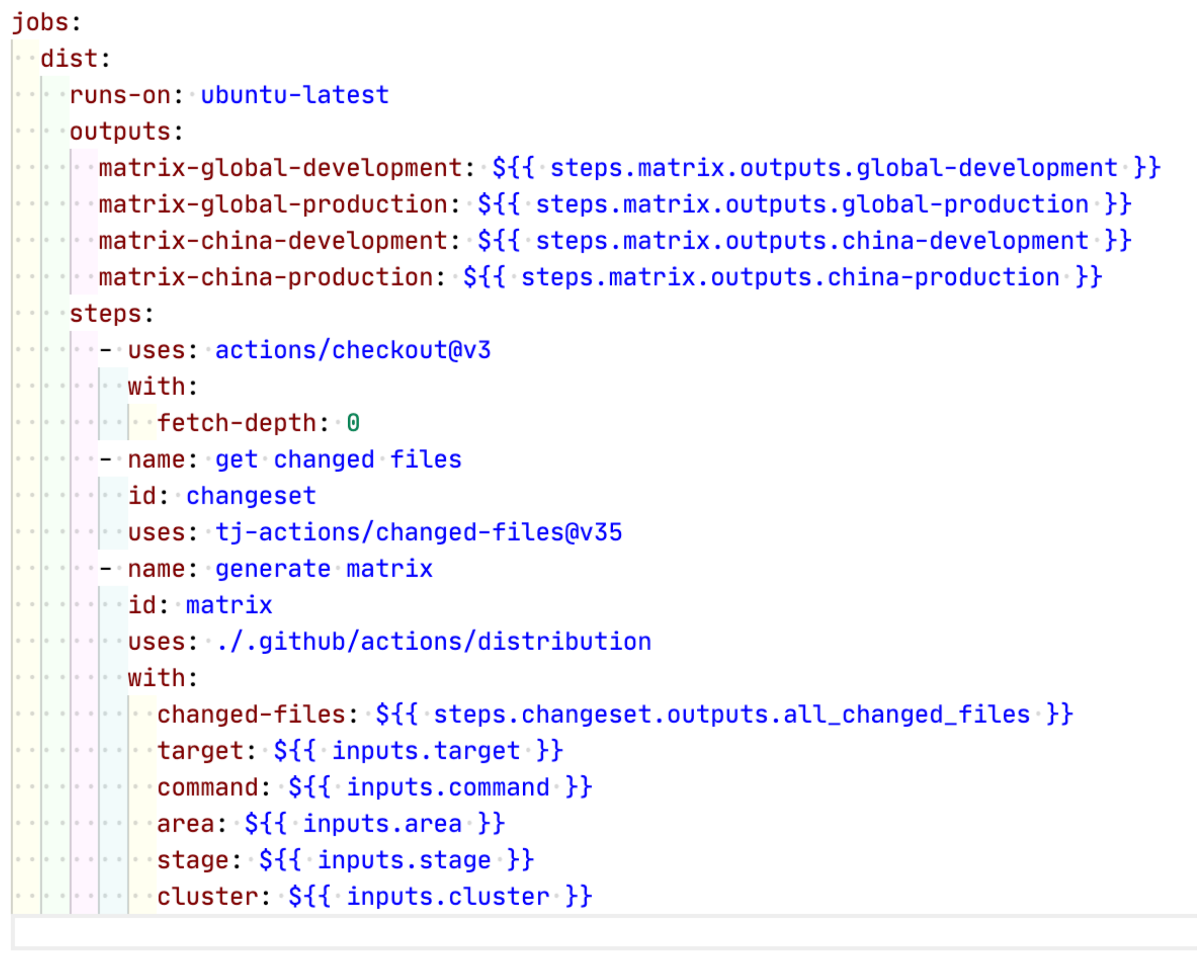
Github Actions

- distribution generation
- actions runner (credentials)
- preview/diff
- release
- notification

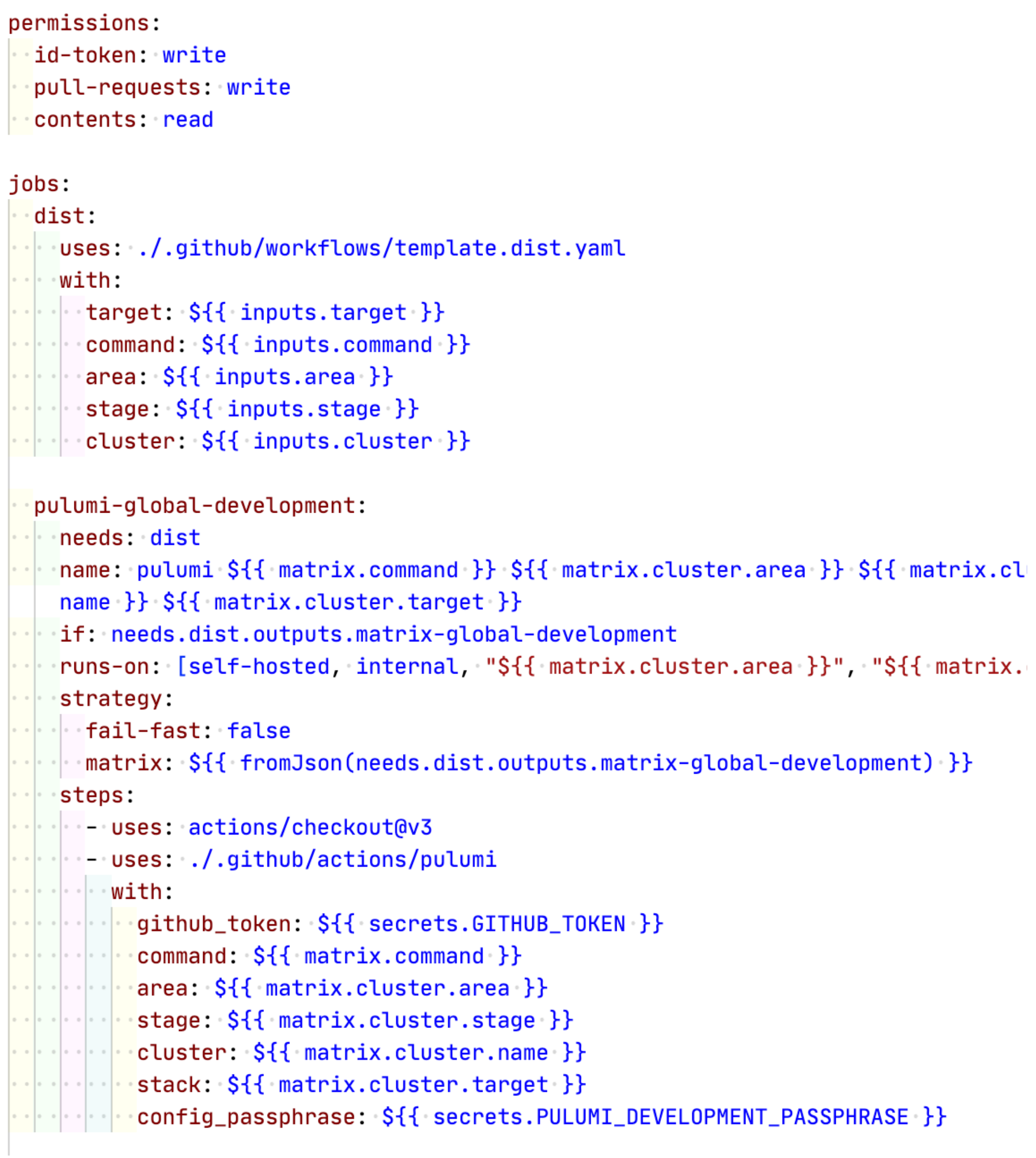
Databend



```yaml
# cluster name ref: https://www.w3.org/wiki/CSS/Properties/color/keywords

account: "1234567890"
stage: production
parent: "9876543210"

pulumi:
  account: "9876543210"
  backend_url: s3://management/pulumi/development
  secrets_provider: awskms:///arn:aws:kms:us-east-2:9876543210:key/4aaccd6

director:
  name: silver
  platform: aws
  region: us-east-2
  cidr: 10.1.0.0/16
  is_director: true

clusters: []
  # - name: cyan
  #   platform: aws
  #   region: us-east-1
  #   cidr: 10.2.0.0/16

  # - name: lime
  #   provider: azure
  #   region: westus3
  #   cidr: 10.11.0.0/16
  #   pending: true

  # - name: aqua
  #   provider: gcp
  #   region: us-central1-b
  #   cidr: 10.12.0.0/16
```

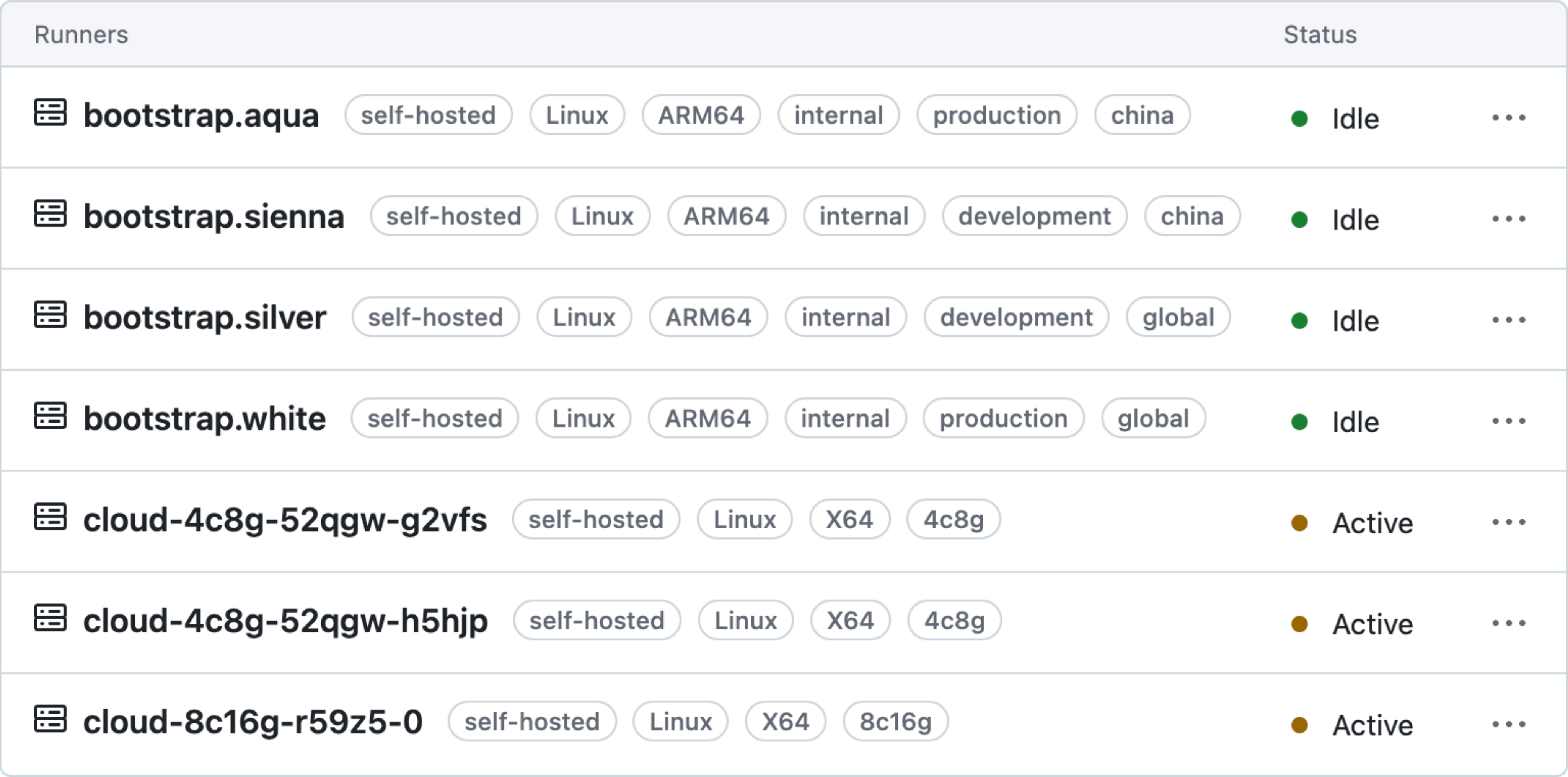


```yaml
jobs:
  dist:
    runs-on: ubuntu-latest
    outputs:
      matrix-global-development: ${{ steps.matrix.outputs.global-development }}
      matrix-global-production: ${{ steps.matrix.outputs.global-production }}
      matrix-china-development: ${{ steps.matrix.outputs.china-development }}
      matrix-china-production: ${{ steps.matrix.outputs.china-production }}
    steps:
      - uses: actions/checkout@v3
        with:
          fetch-depth: 0
      - name: get changed files
        id: changeset
        uses: tj-actions/changed-files@v35
      - name: generate matrix
        id: matrix
        uses: ./.github/actions/distribution
        with:
          changed-files: ${{ steps.changeset.outputs.all_changed_files }}
          target: ${{ inputs.target }}
          command: ${{ inputs.command }}
          area: ${{ inputs.area }}
          stage: ${{ inputs.stage }}
          cluster: ${{ inputs.cluster }}
```

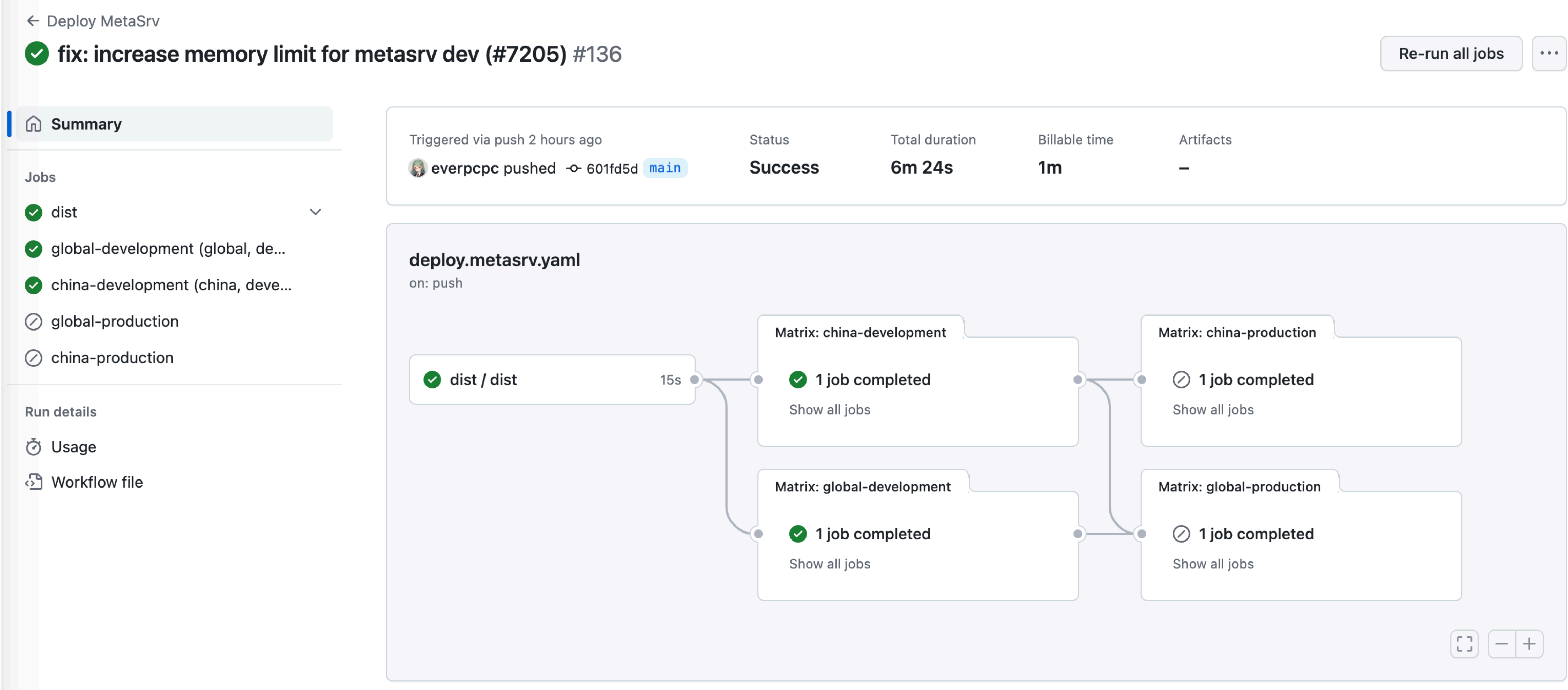


```yaml
permissions:
  id-token: write
  pull-requests: write
  contents: read

jobs:
  dist:
    uses: ./.github/workflows/template.dist.yaml
    with:
      target: ${{ inputs.target }}
      command: ${{ inputs.command }}
      area: ${{ inputs.area }}
      stage: ${{ inputs.stage }}
      cluster: ${{ inputs.cluster }}

  pulumi-global-development:
    needs: dist
    name: pulumi ${{ matrix.command }} ${{ matrix.cluster.area }} ${{ matrix.cl
    name }} ${{ matrix.cluster.target }}
    if: needs.dist.outputs.matrix-global-development
    runs-on: [self-hosted, internal, "${{ matrix.cluster.area }}", "${{ matrix.
    strategy:
      fail-fast: false
      matrix: ${{ fromJson(needs.dist.outputs.matrix-global-development) }}
    steps:
      - uses: actions/checkout@v3
      - uses: ./.github/actions/pulumi
        with:
          github_token: ${{ secrets.GITHUB_TOKEN }}
          command: ${{ matrix.command }}
          area: ${{ matrix.cluster.area }}
          stage: ${{ matrix.cluster.stage }}
          cluster: ${{ matrix.cluster.name }}
          stack: ${{ matrix.cluster.target }}
          config_passphrase: ${{ secrets.PULUMI_DEVELOPMENT_PASSPHRASE }}
```

Databend



Runners		Status
bootstrap.aqua	self-hosted Linux ARM64 internal production china	● Idle
bootstrap.sienna	self-hosted Linux ARM64 internal development china	● Idle
bootstrap.silver	self-hosted Linux ARM64 internal development global	● Idle
bootstrap.white	self-hosted Linux ARM64 internal production global	● Idle
cloud-4c8g-52qgw-g2vfs	self-hosted Linux X64 4c8g	● Active
cloud-4c8g-52qgw-h5hjp	self-hosted Linux X64 4c8g	● Active
cloud-8c16g-r59z5-0	self-hosted Linux X64 8c16g	● Active

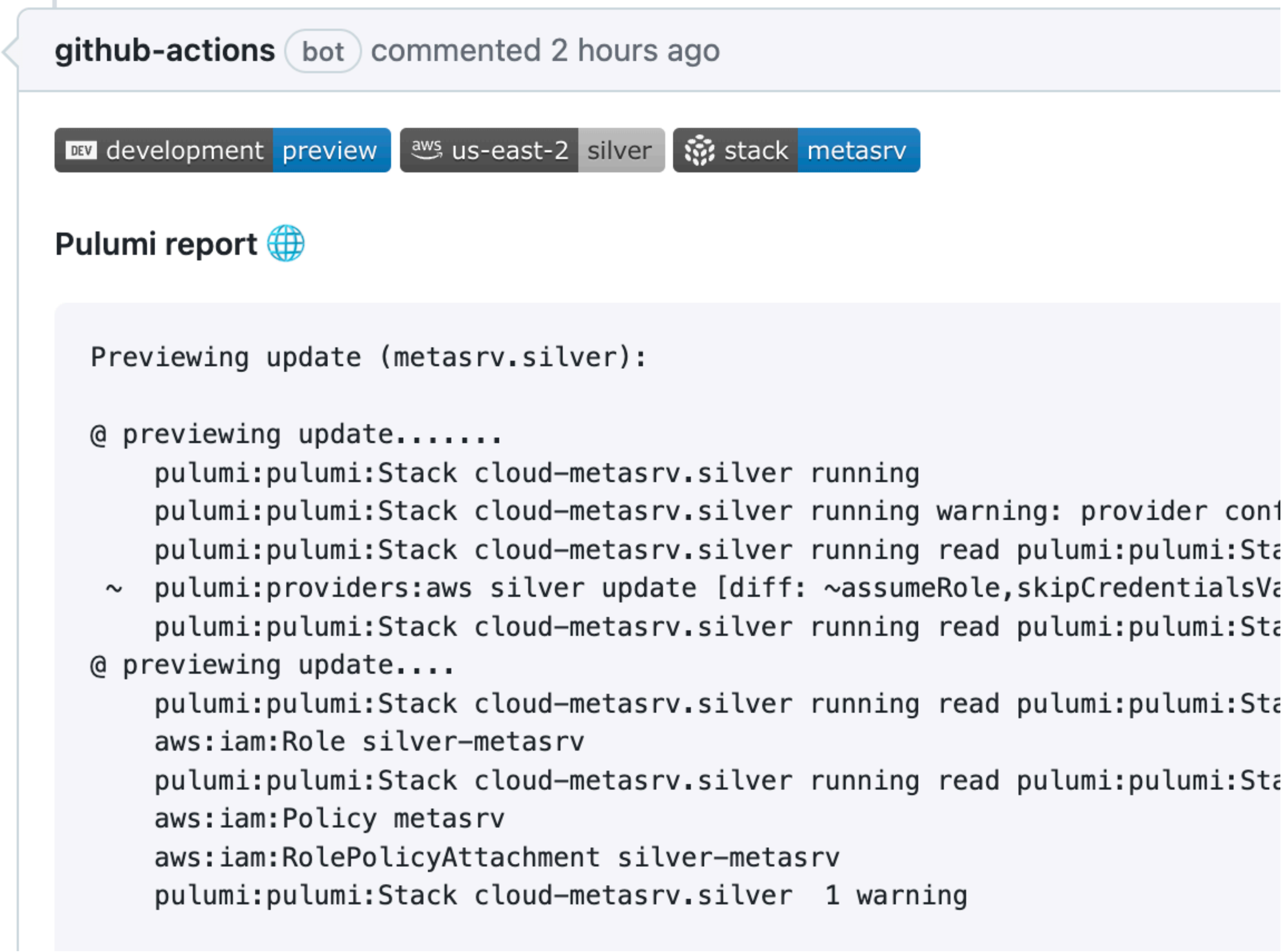


← Deploy MetaSrv

✓ fix: increase memory limit for metasrv dev (#7205) #136

Triggered via push 2 hours ago	Status	Total duration	Billable time	Artifacts
everpcpc pushed 601fd5d main	Success	6m 24s	1m	–

deploy.metasrv.yaml
on: push

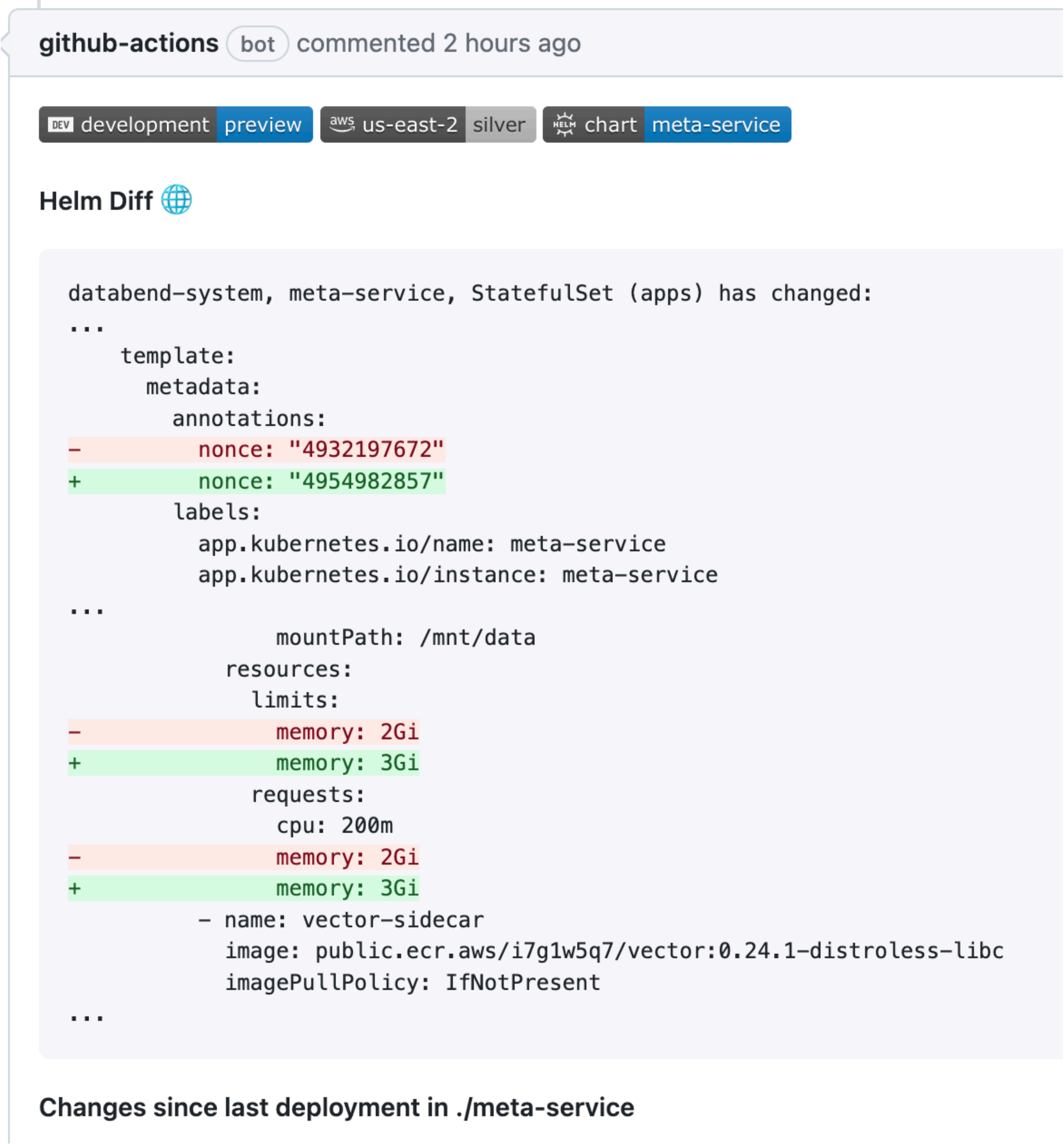


github-actions bot commented 2 hours ago

DEV development preview | aws us-east-2 silver | stack metasrv

Pulumi report 🌐

```
Previewing update (metasrv.silver):

@ previewing update.......
  pulumi:pulumi:Stack cloud-metasrv.silver running
  pulumi:pulumi:Stack cloud-metasrv.silver running warning: provider conf
  pulumi:pulumi:Stack cloud-metasrv.silver running read pulumi:pulumi:Sta
~ pulumi:providers:aws silver update [diff: ~assumeRole,skipCredentialsVa
  pulumi:pulumi:Stack cloud-metasrv.silver running read pulumi:pulumi:Sta
@ previewing update....
  pulumi:pulumi:Stack cloud-metasrv.silver running read pulumi:pulumi:Sta
  aws:iam:Role silver-metasrv
  pulumi:pulumi:Stack cloud-metasrv.silver running read pulumi:pulumi:Sta
  aws:iam:Policy metasrv
  aws:iam:RolePolicyAttachment silver-metasrv
  pulumi:pulumi:Stack cloud-metasrv.silver  1 warning
```



github-actions bot commented 2 hours ago

DEV development preview | aws us-east-2 silver | HELM chart meta-service

Helm Diff 🌐

```
databend-system, meta-service, StatefulSet (apps) has changed:
...
  template:
   metadata:
    annotations:
-    nonce: "4932197672"
+    nonce: "4954982857"
    labels:
     app.kubernetes.io/name: meta-service
     app.kubernetes.io/instance: meta-service
...
        mountPath: /mnt/data
      resources:
       limits:
-       memory: 2Gi
+       memory: 3Gi
       requests:
        cpu: 200m
-       memory: 2Gi
+       memory: 3Gi
     - name: vector-sidecar
      image: public.ecr.aws/i7g1w5q7/vector:0.24.1-distroless-libc
      imagePullPolicy: IfNotPresent
...
```

Changes since last deployment in ./meta-service

Databend

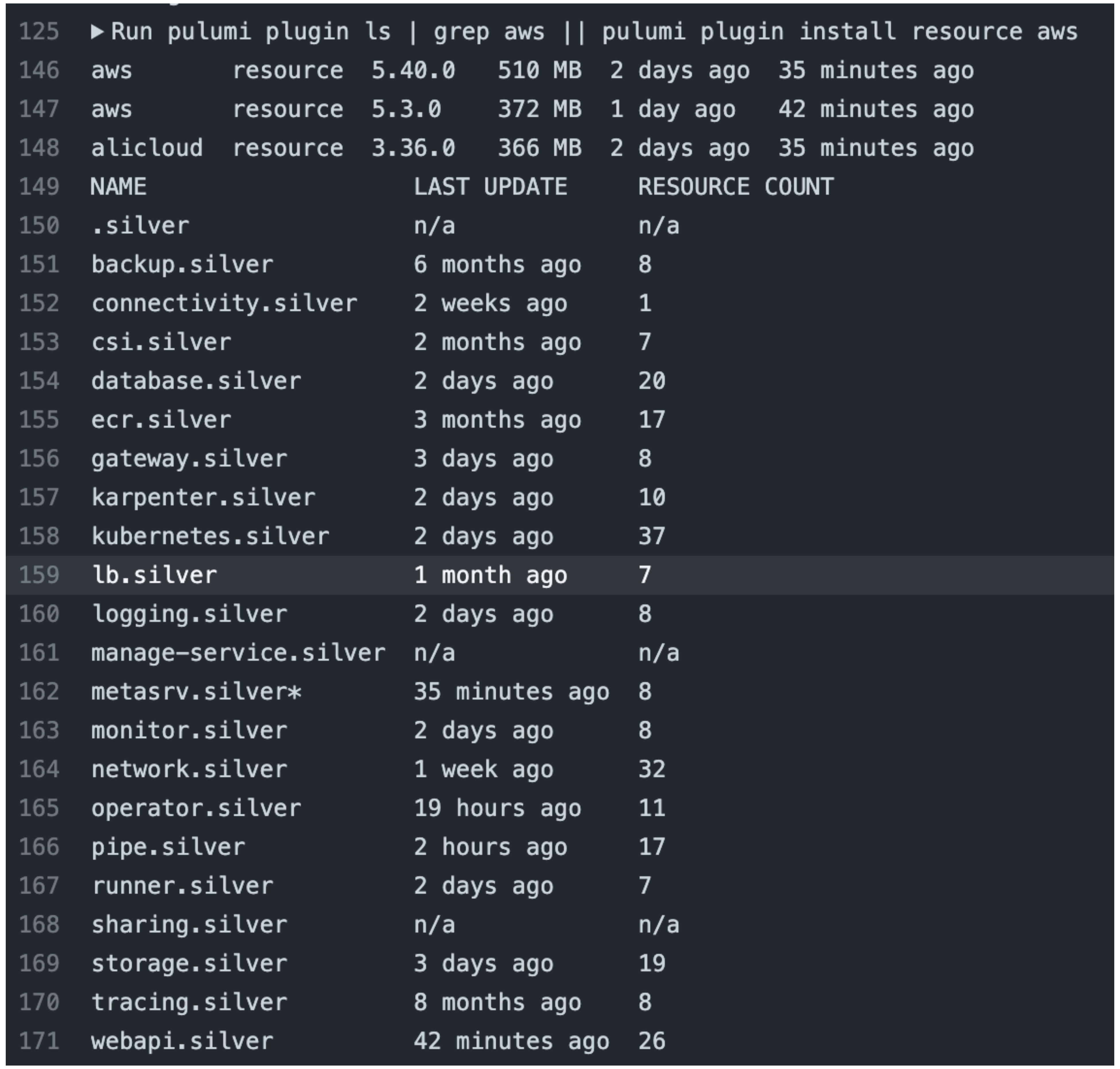
Part 3

在使用过程中遇到的问题

慢！

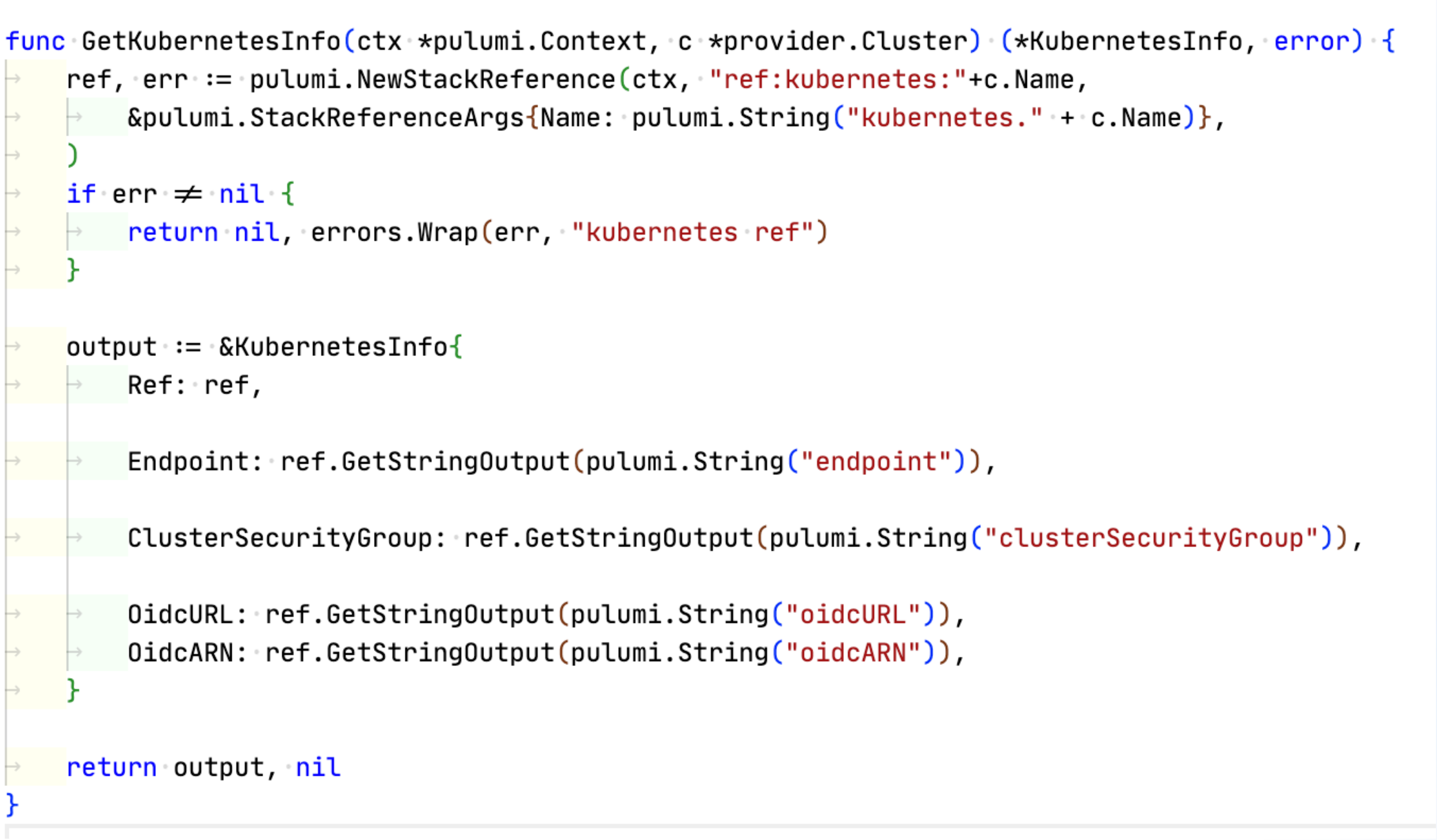
Databend

Stack 拆分



```
▶ Run pulumi plugin ls | grep aws || pulumi plugin install resource aws
aws       resource  5.40.0   510 MB  2 days ago  35 minutes ago
aws       resource  5.3.0    372 MB  1 day ago   42 minutes ago
alicloud  resource  3.36.0   366 MB  2 days ago  35 minutes ago
NAME                    LAST UPDATE     RESOURCE COUNT
.silver                 n/a             n/a
backup.silver           6 months ago    8
connectivity.silver     2 weeks ago     1
csi.silver              2 months ago    7
database.silver         2 days ago      20
ecr.silver              3 months ago    17
gateway.silver          3 days ago      8
karpenter.silver        2 days ago      10
kubernetes.silver       2 days ago      37
lb.silver               1 month ago     7
logging.silver          2 days ago      8
manage-service.silver   n/a             n/a
metasrv.silver*         35 minutes ago  8
monitor.silver          2 days ago      8
network.silver          1 week ago      32
operator.silver         19 hours ago    11
pipe.silver             2 hours ago     17
runner.silver           2 days ago      7
sharing.silver          n/a             n/a
storage.silver          3 days ago      19
tracing.silver          8 months ago    8
webapi.silver           42 minutes ago  26
```

Stack Reference

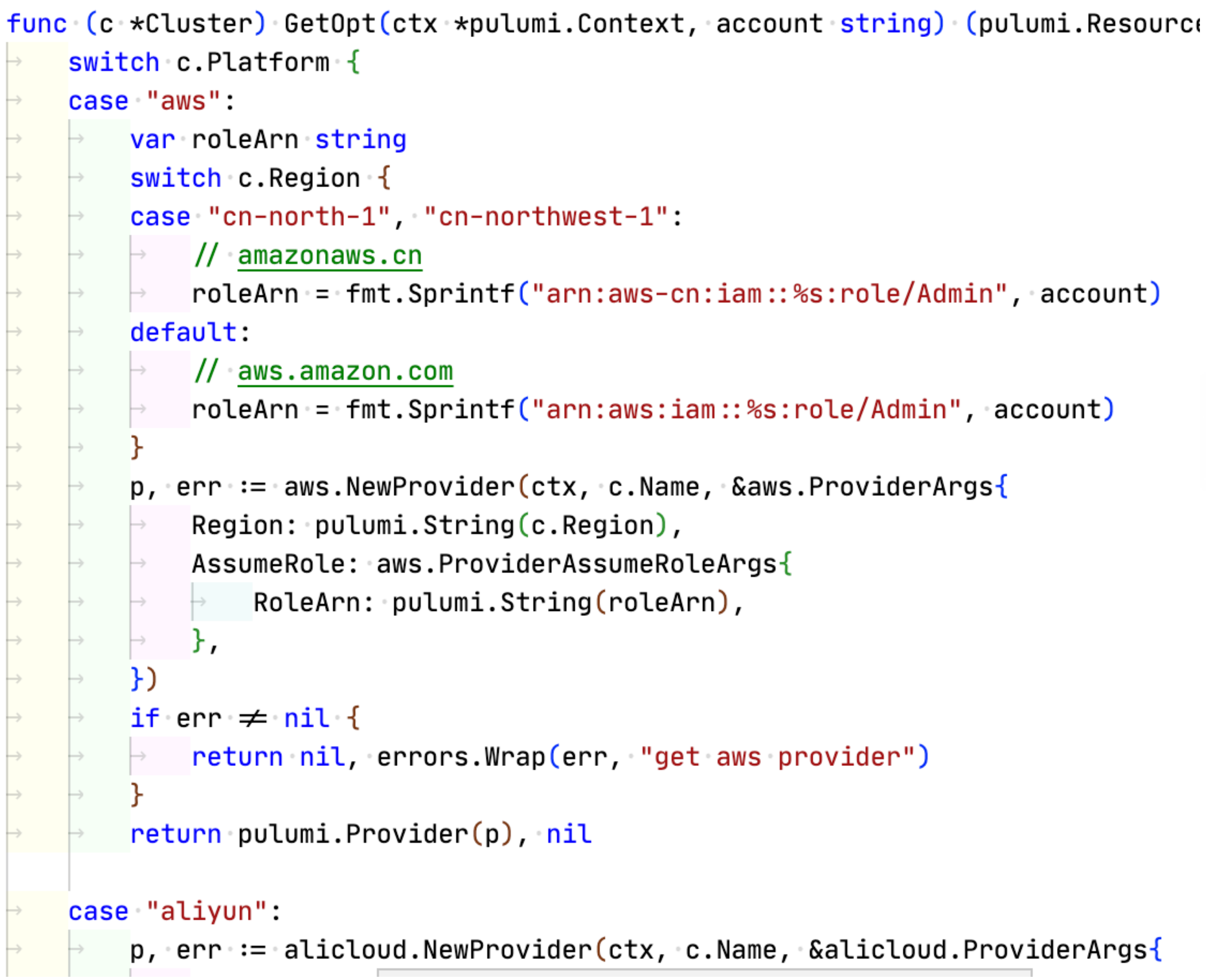


```go
func GetKubernetesInfo(ctx *pulumi.Context, c *provider.Cluster) (*KubernetesInfo, error) {
    ref, err := pulumi.NewStackReference(ctx, "ref:kubernetes:"+c.Name,
        &pulumi.StackReferenceArgs{Name: pulumi.String("kubernetes." + c.Name)},
    )
    if err ≠ nil {
        return nil, errors.Wrap(err, "kubernetes ref")
    }

    output := &KubernetesInfo{
        Ref: ref,

        Endpoint: ref.GetStringOutput(pulumi.String("endpoint")),

        ClusterSecurityGroup: ref.GetStringOutput(pulumi.String("clusterSecurityGroup")),

        OidcURL: ref.GetStringOutput(pulumi.String("oidcURL")),
        OidcARN: ref.GetStringOutput(pulumi.String("oidcARN")),
    }

    return output, nil
}
```

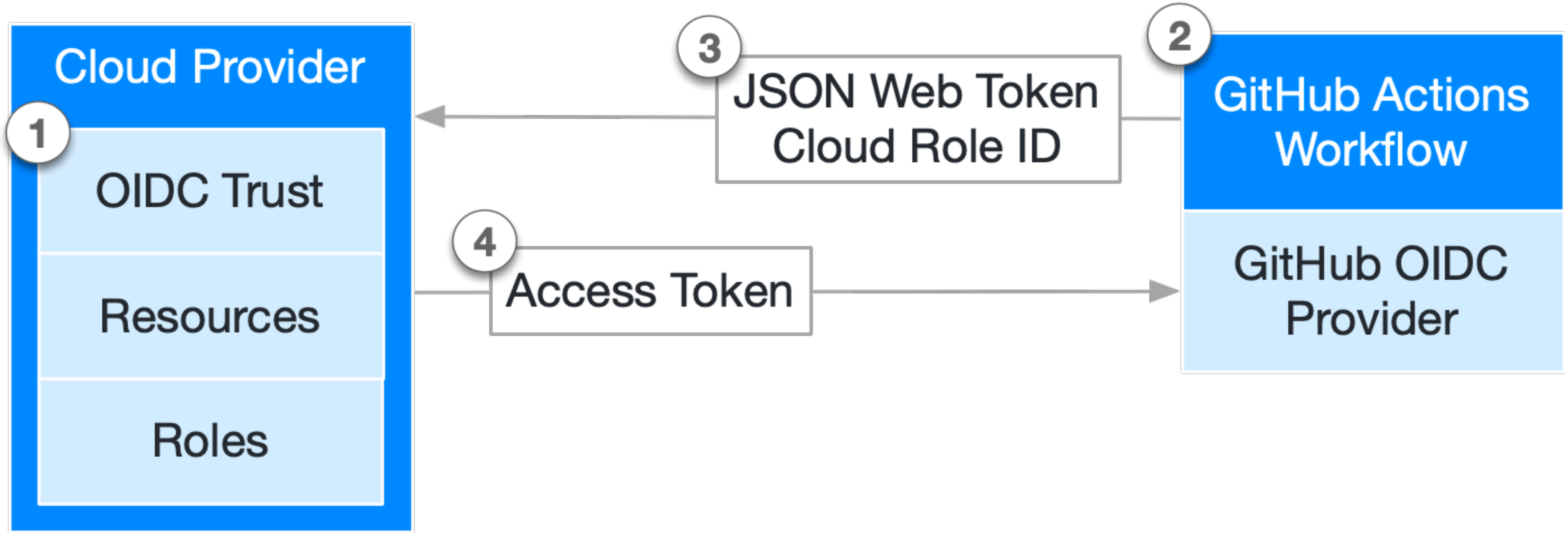
Databend

权限！

Provider



```go
func (c *Cluster) GetOpt(ctx *pulumi.Context, account string) (pulumi.Resourc
    switch c.Platform {
    case "aws":
        var roleArn string
        switch c.Region {
        case "cn-north-1", "cn-northwest-1":
            // amazonaws.cn
            roleArn = fmt.Sprintf("arn:aws-cn:iam::%s:role/Admin", account)
        default:
            // aws.amazon.com
            roleArn = fmt.Sprintf("arn:aws:iam::%s:role/Admin", account)
        }
        p, err := aws.NewProvider(ctx, c.Name, &aws.ProviderArgs{
            Region: pulumi.String(c.Region),
            AssumeRole: aws.ProviderAssumeRoleArgs{
                RoleArn: pulumi.String(roleArn),
            },
        })
        if err ≠ nil {
            return nil, errors.Wrap(err, "get aws provider")
        }
        return pulumi.Provider(p), nil

    case "aliyun":
        p, err := alicloud.NewProvider(ctx, c.Name, &alicloud.ProviderArgs{
```



Cloud Provider

1 OIDC Trust

Resources

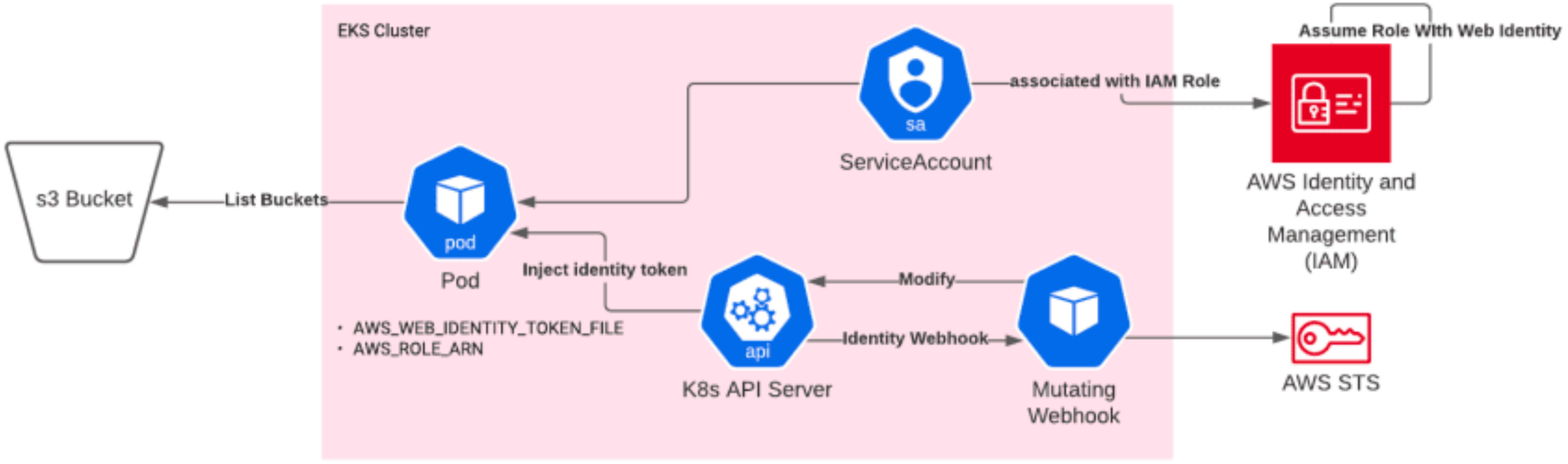
Roles

2 GitHub Actions Workflow

GitHub OIDC Provider

3 JSON Web Token Cloud Role ID

4 Access Token



Part 4

总结

Thank you！