MesosCon
EUROPE

mesos2iam

Zain Malik / Software Engineer / Schibsted Media Group

THE LINUX FOUNDATION

Schibsted Media Group

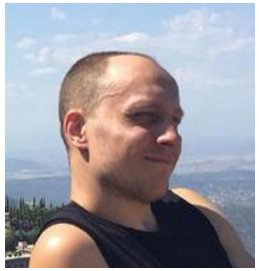
- 22 countries
- 38 products
- 1.2bn people
- 30m+ daily users

SCHIBSTED MEDIA GROUP

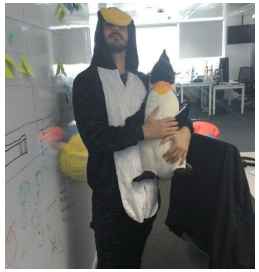
THE LINUX FOUNDATION

Team

Fabian Selles

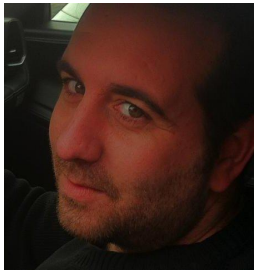


Ivan Ilves



Alan Bover

Sergi Mansilla



Jaime Jorge

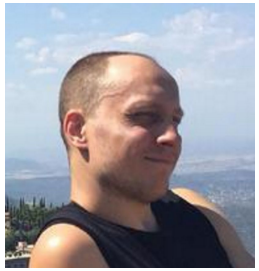
Zain Malik

SCHIBSTED MEDIA GROUP

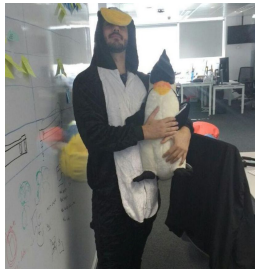
THE LINUX FOUNDATION

Team

Fabian Selles

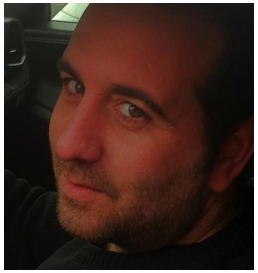


Ivan Ilves



Alan Bover

Sergi Mansilla



Jaime Jorge

Zain Malik

Contributor

Vicent Soria

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team

CRE (common runtime environments)

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team

CRE (common runtime environments)

>6K tasks

>15k jobs

>2k pods

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team

CRE (common runtime environments)

>6K tasks / day
>8GB / task
>1.4 cpu/task
~50 minutes

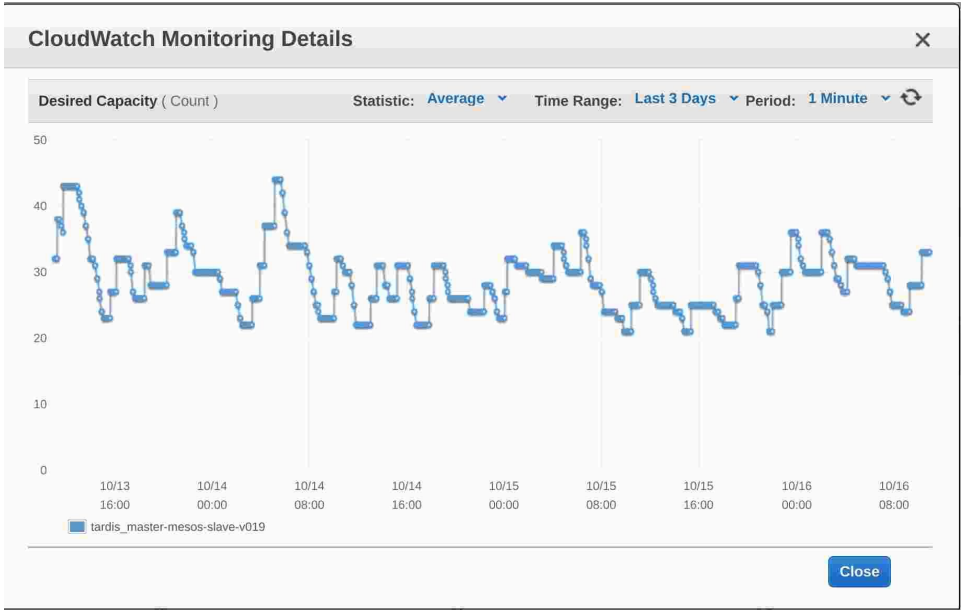
>15k jobs

>2k pods

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team

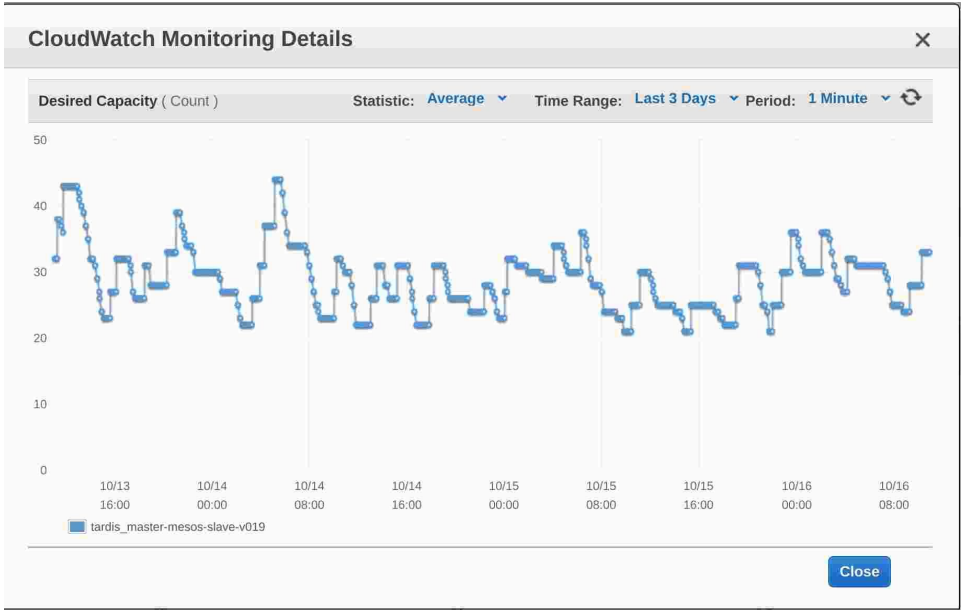


scaling down cluster with 0 failed task

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team



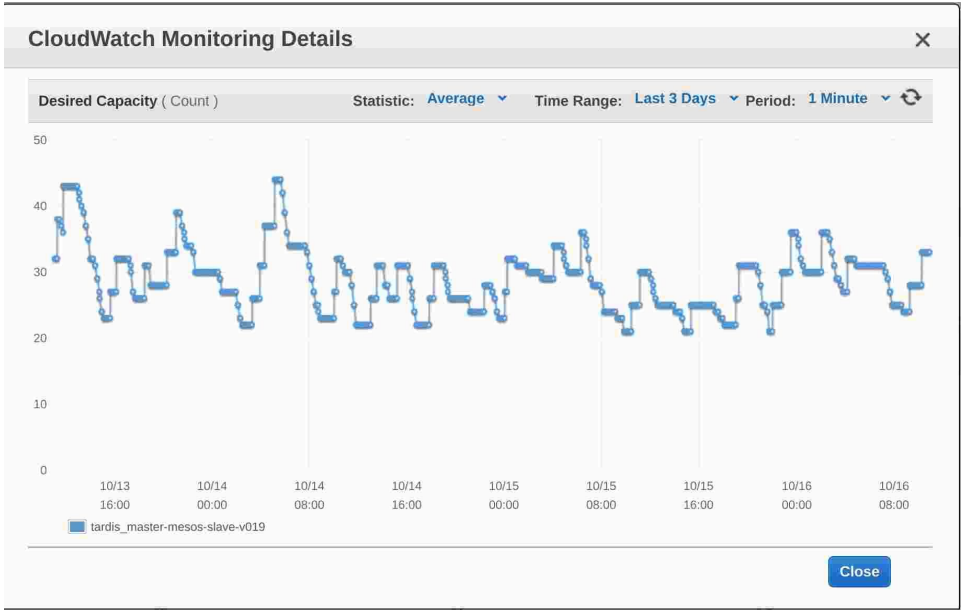
scaling down cluster with 0 failed task

The creepy guys who track down all frameworks we use and ask them to implement mesos maintenance primitives

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team



scaling down cluster with 0 failed task

The creepy guys who track down all frameworks we use and ask them to implement mesos maintenance primitives

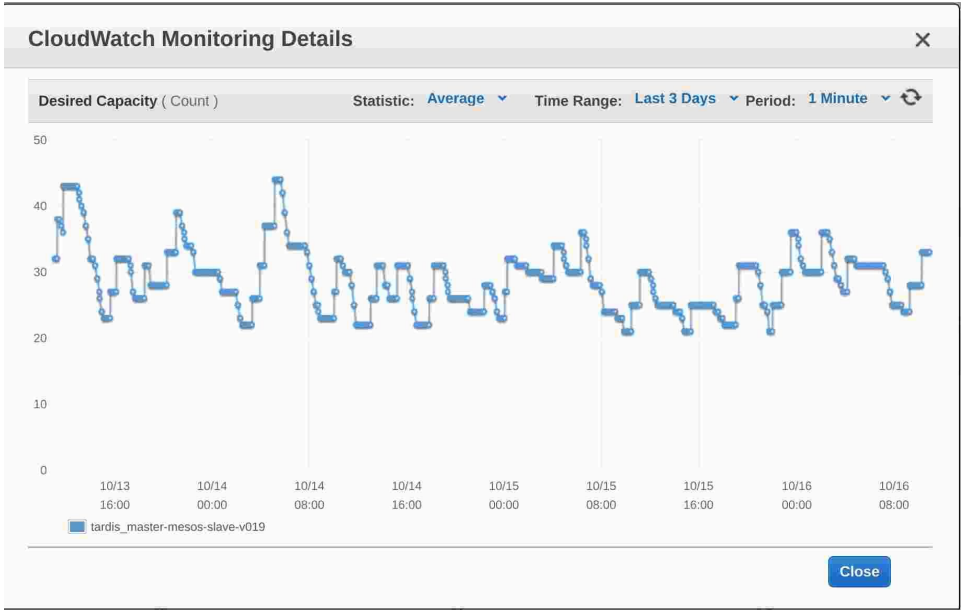
CHR

eremetic

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Team



scaling down cluster with 0 failed task

The creepy guys who track down all frameworks we use and ask them to implement mesos maintenance primitives

fyi: deathnode → https://github.com/alanbover/deathnode

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

mesos2**iam**

THE LINUX FOUNDATION

IAM

- Stands for “Identity and Access Management”
- Takes care of Who(authentication) and How(authorization)

SCHIBSTED MEDIA GROUP
THE LINUX FOUNDATION

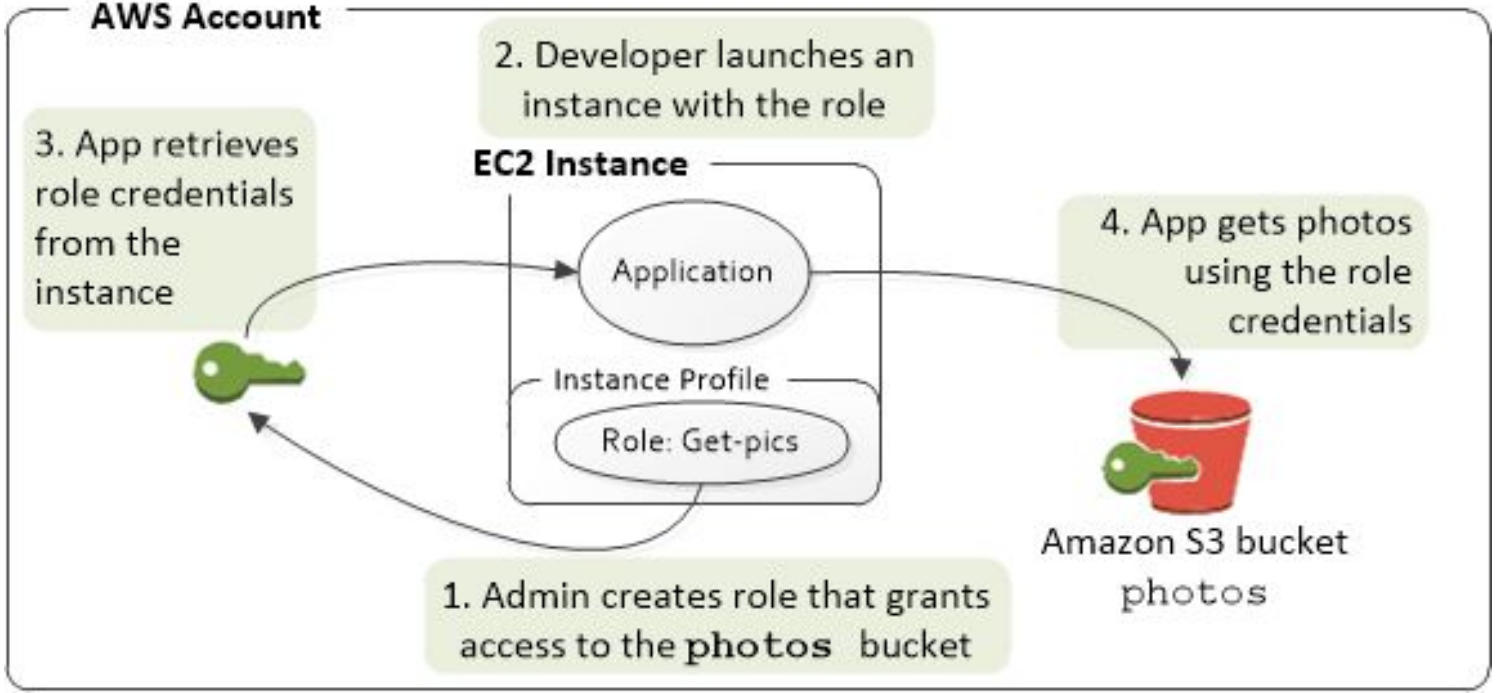
IAM

- Action-level permissions
- Resource-level permissions
- Resource-based permissions
- Tag-based permissions
- Temporary security credentials
- Service-linked roles

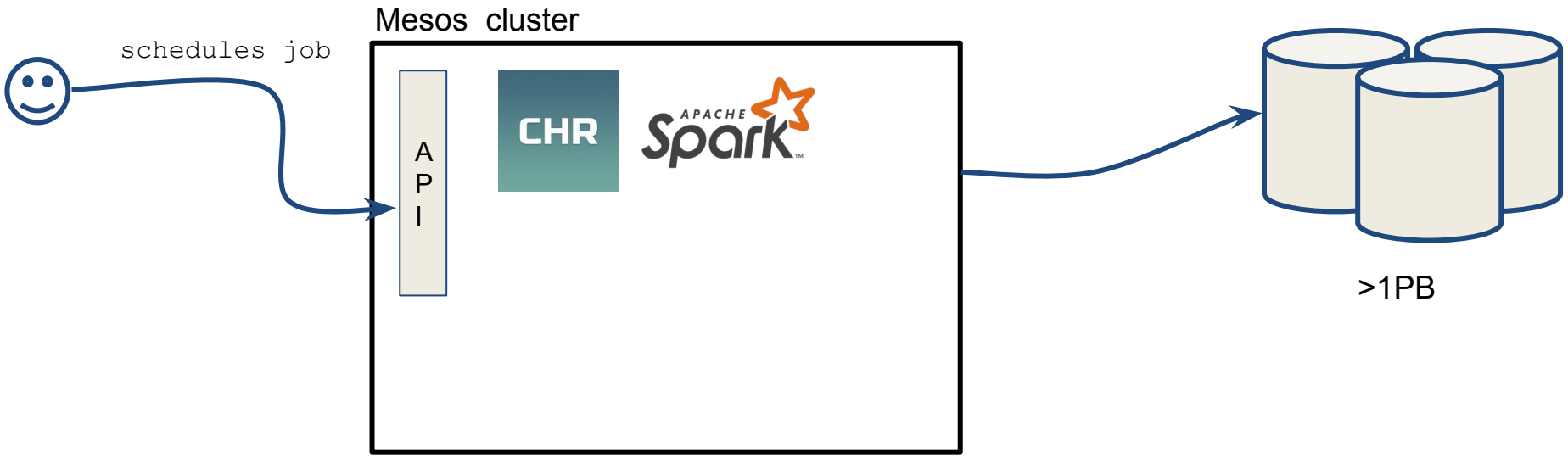
SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

IAM with instances

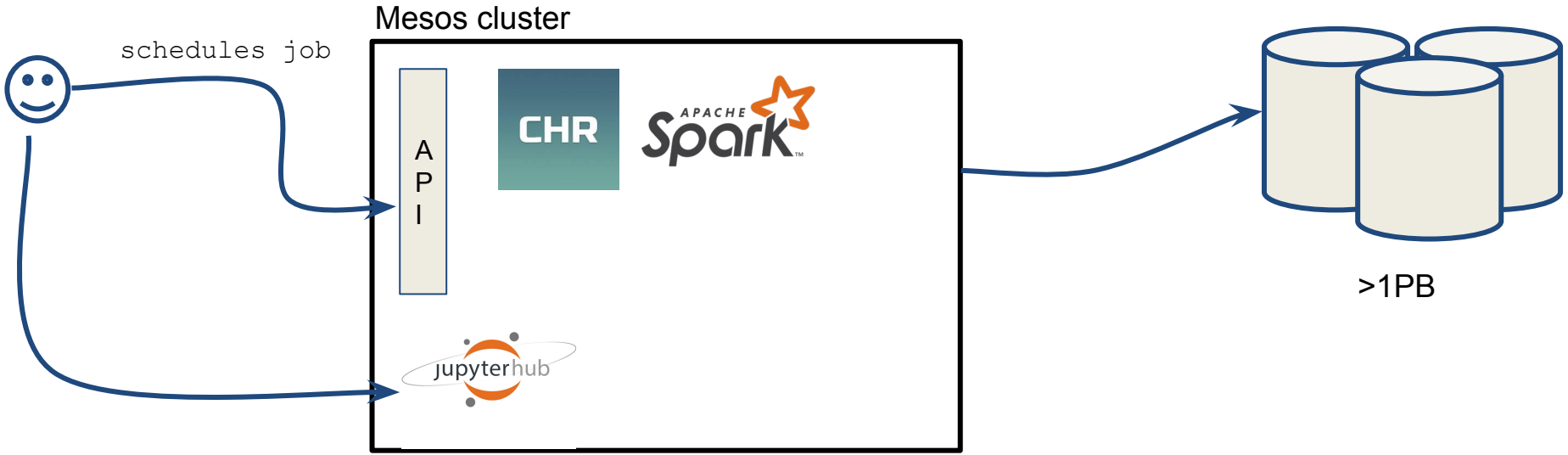


Our use case



>6k daily tasks

Our use case

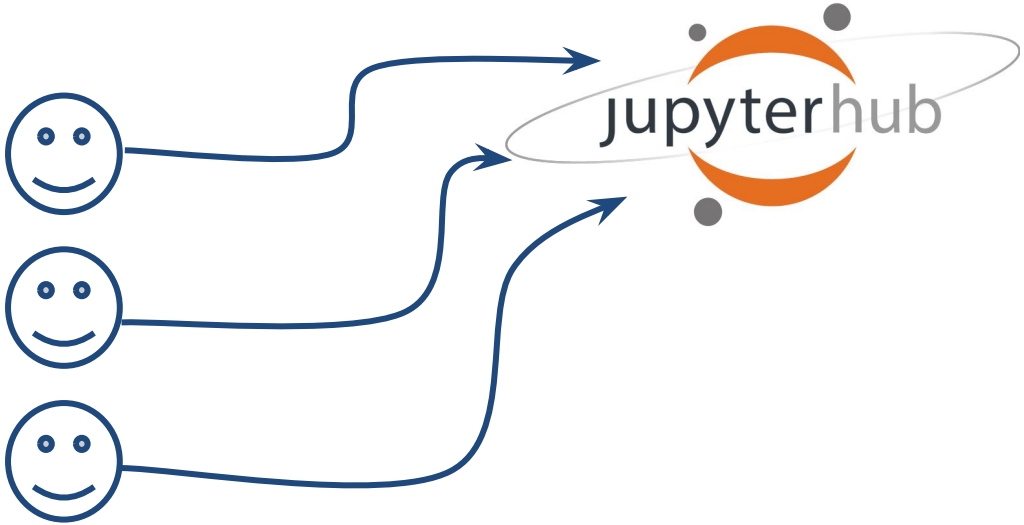


>6k daily tasks

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

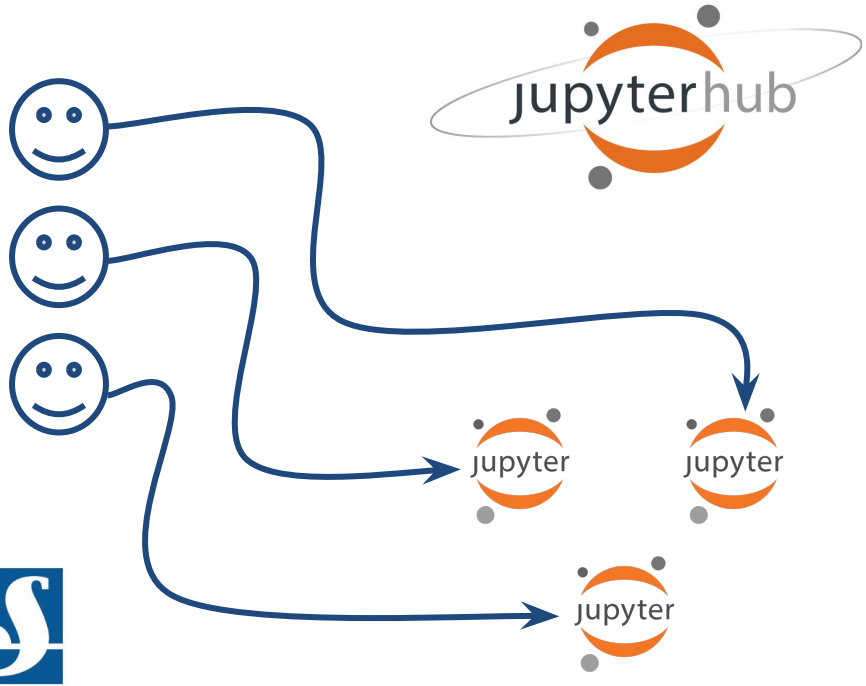
Our use case



SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

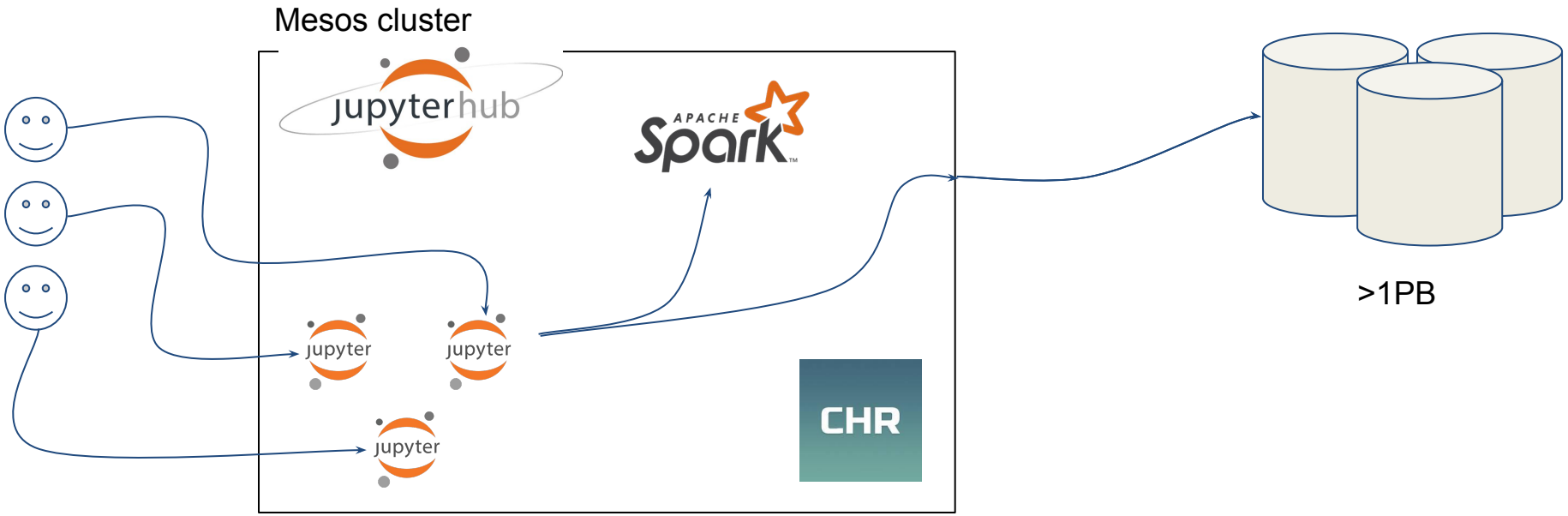
Our use case



SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

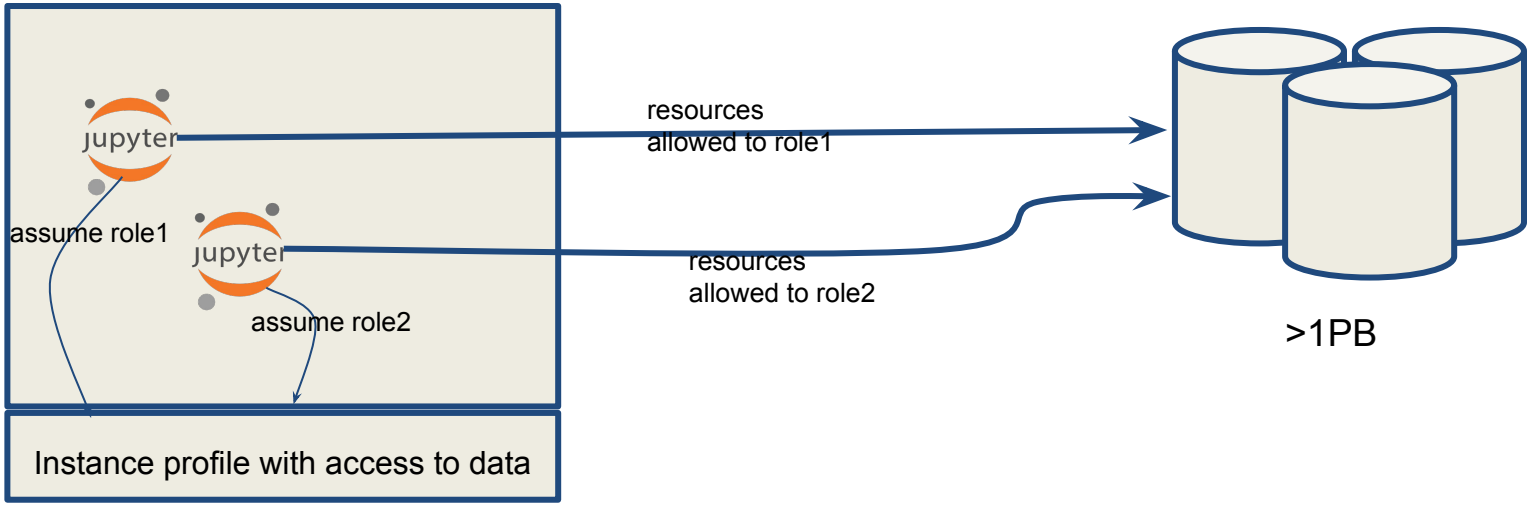
Our use case



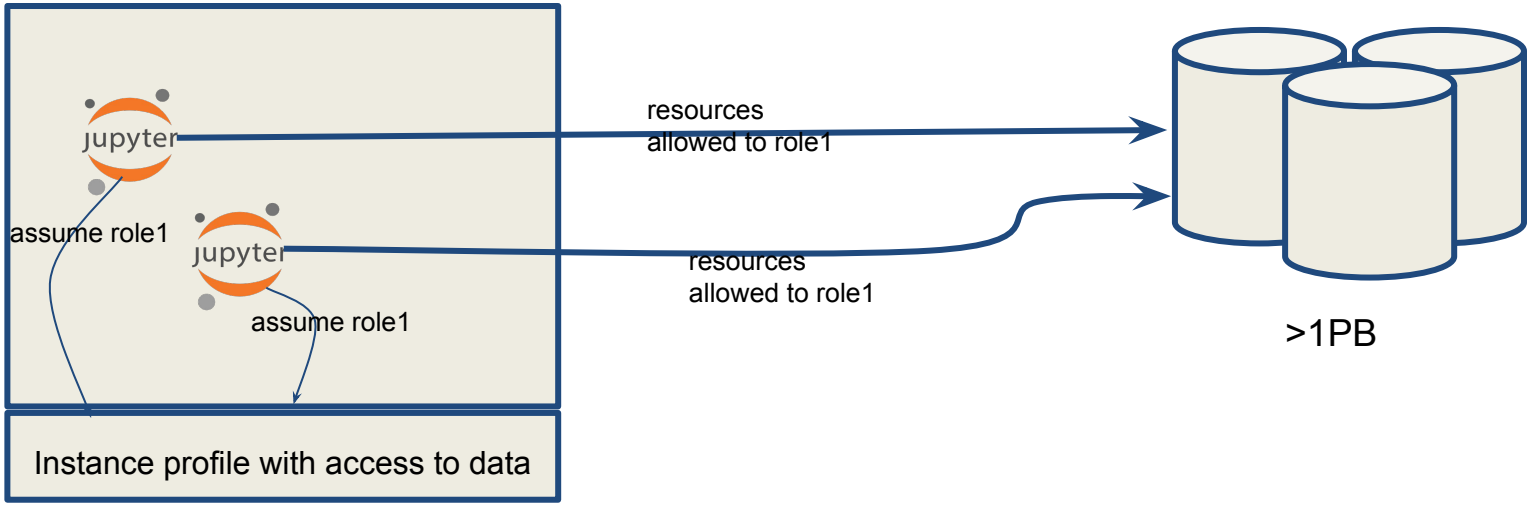
SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

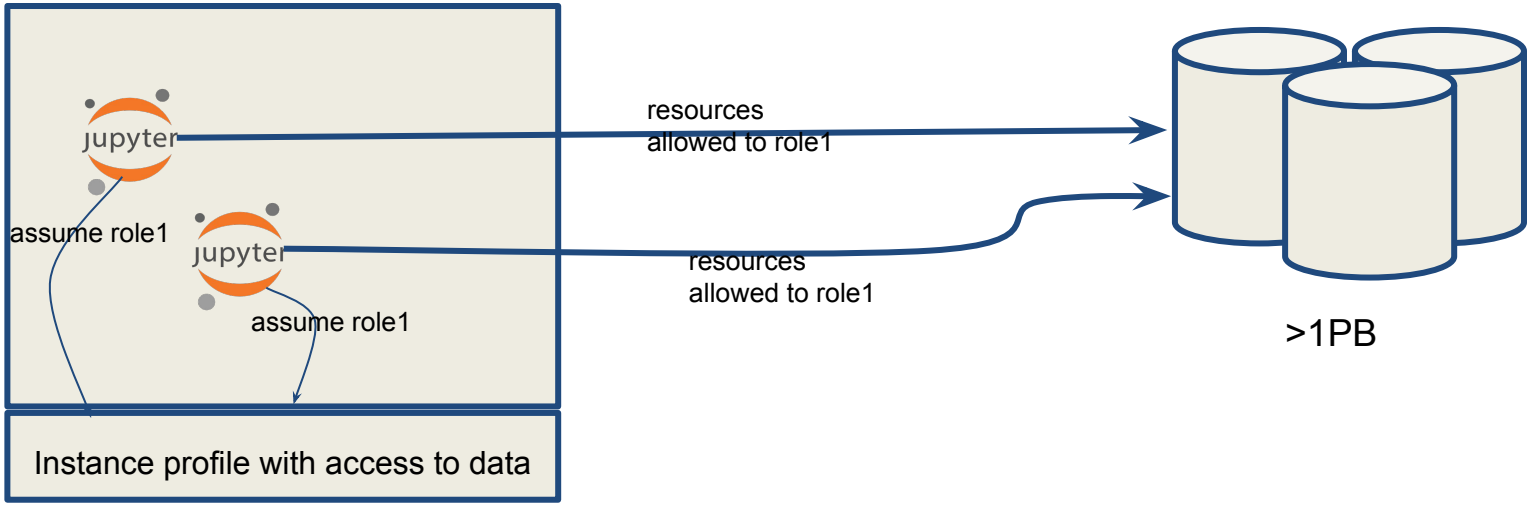
Our use case


jupyter
assume role1
jupyter
assume role2
Instance profile with access to data
resources
allowed to role1
resources
allowed to role2
>1PB

Our use case


jupyter
assume role1
jupyter
assume role1
Instance profile with access to data
resources
allowed to role1
resources
allowed to role1
>1PB

Our use case

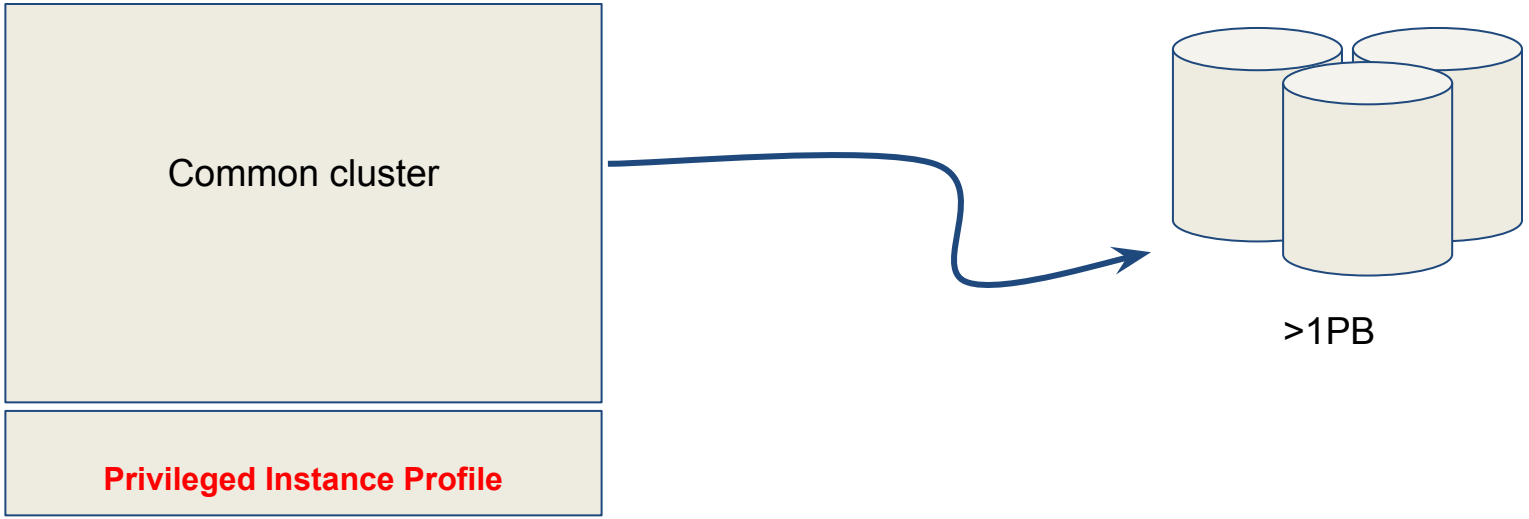


Problem? Each user just need to know the other users iam role, create a job with other role and access those resources

SCHIBSTED
MEDIA GROUP

THE LINUX FOUNDATION

The problem



iam

let’s dig deep

THE LINUX FOUNDATION

IAM

How do EC2 instances retrieve their credentials?

1. 169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI
2. 169.254.169.254/latest/meta-data/iam/security-credentials/$ROLE

From version 1.11.0 in all AWS sdk clients it goes through the 1st option*

*If it's set AWS_CONTAINER_CREDENTIALS_RELATIVE_URI, the client send the request to http://169.254.170.2${AWS_CONTAINER_CREDENTIALS_RELATIVE_URI} instead of the usual /latest/meta-data/iam/security-credentials

THE LINUX FOUNDATION

IAM

Actually that's how IAM roles for ECS tasks are working

```
the ECS Agent populates the
AWS_CONTAINER_CREDENTIALS_RELATIVE_URI variable
With /credential_provider_version/credentials?id=task_UUID
```

in other words
169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI
is
169.254.170.2/*credential_provider_version*/credentials?id=*task_UUID*

THE LINUX FOUNDATION

IAM in Action

```
$> curl 169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI
$> {
   "AccessKeyId": "ACCESS_KEY_ID",
   "Expiration": "EXPIRATION_DATE",
   "RoleArn": "TASK_ROLE_ARN",
   "SecretAccessKey": "SECRET_ACCESS_KEY",
   "Token": "SECURITY_TOKEN_STRING"
}
```

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

mesos2iam

THE LINUX FOUNDATION

mesos2iam

mesos2iam is a daemon that runs inside Mesos agents

To give us back the control of IAM policies on tasks level

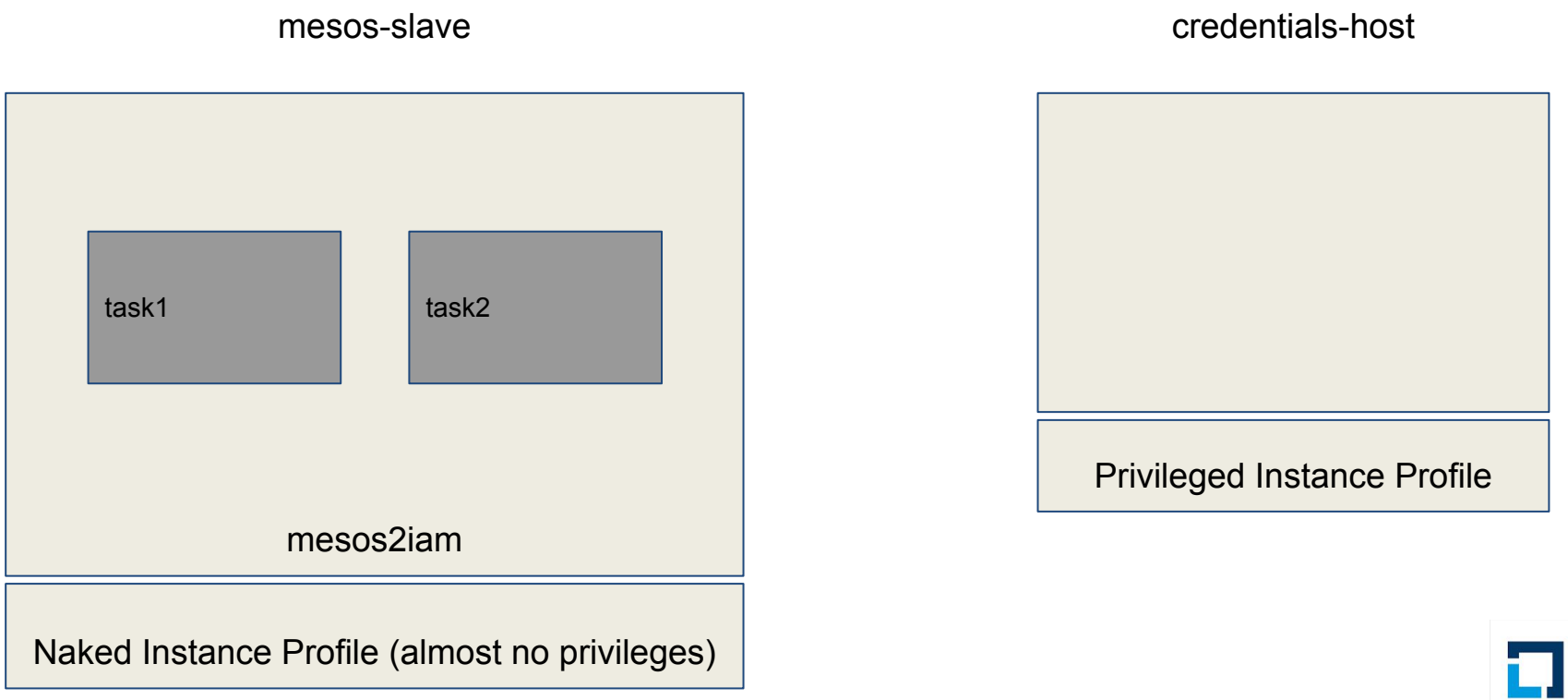
SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

mesos2iam

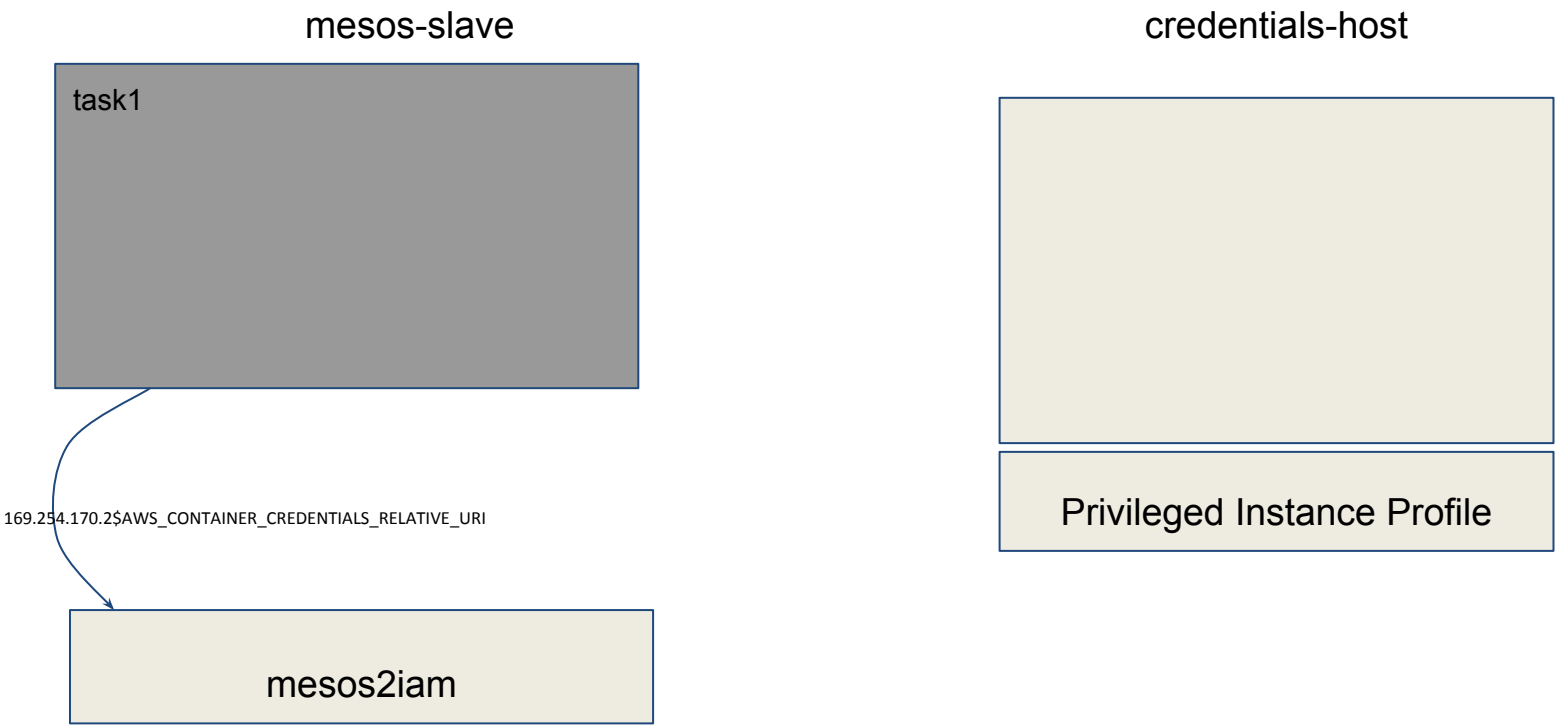
- manage iptables rules
- retrieve a *TASK ID* from container
- fetch credentials for the task

mesos2iam



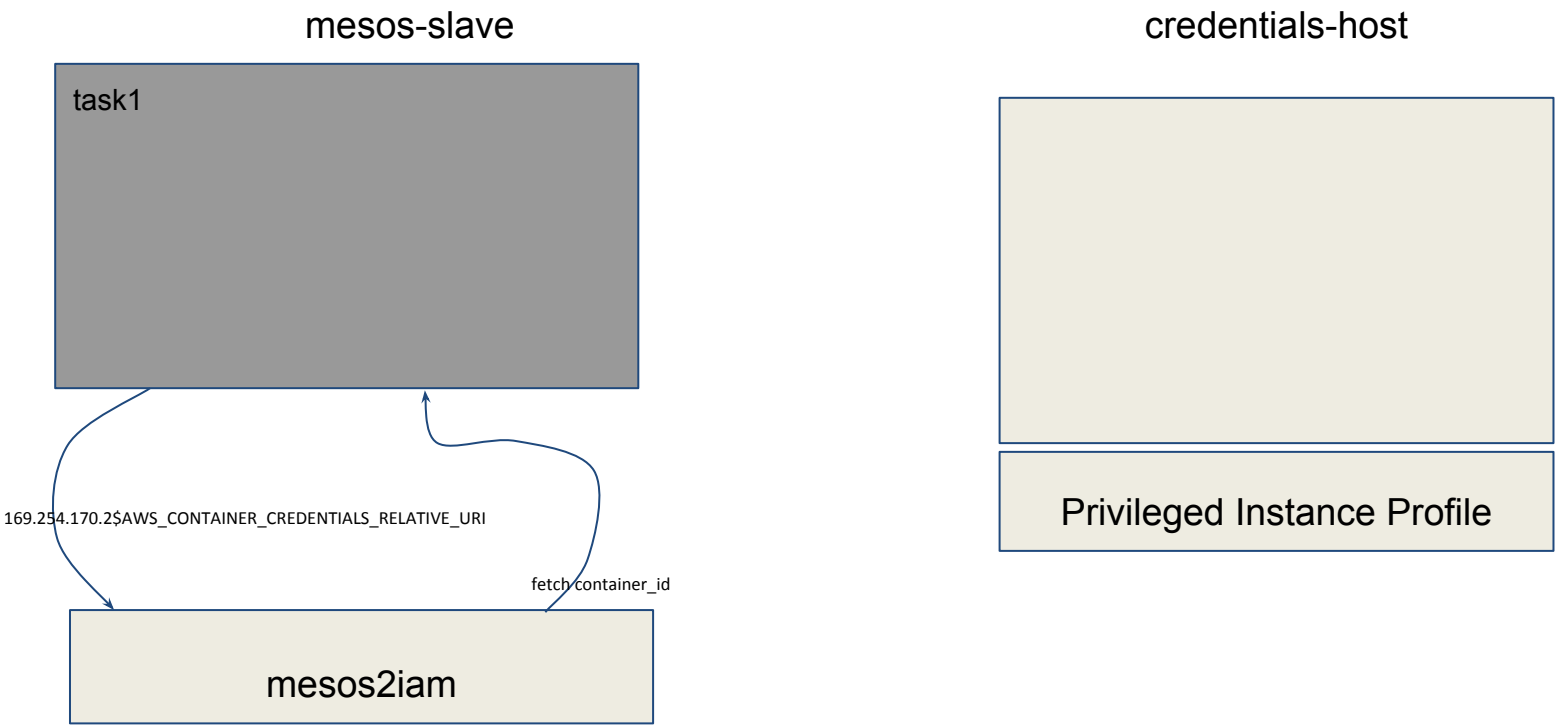
THE LINUX FOUNDATION

mesos2iam



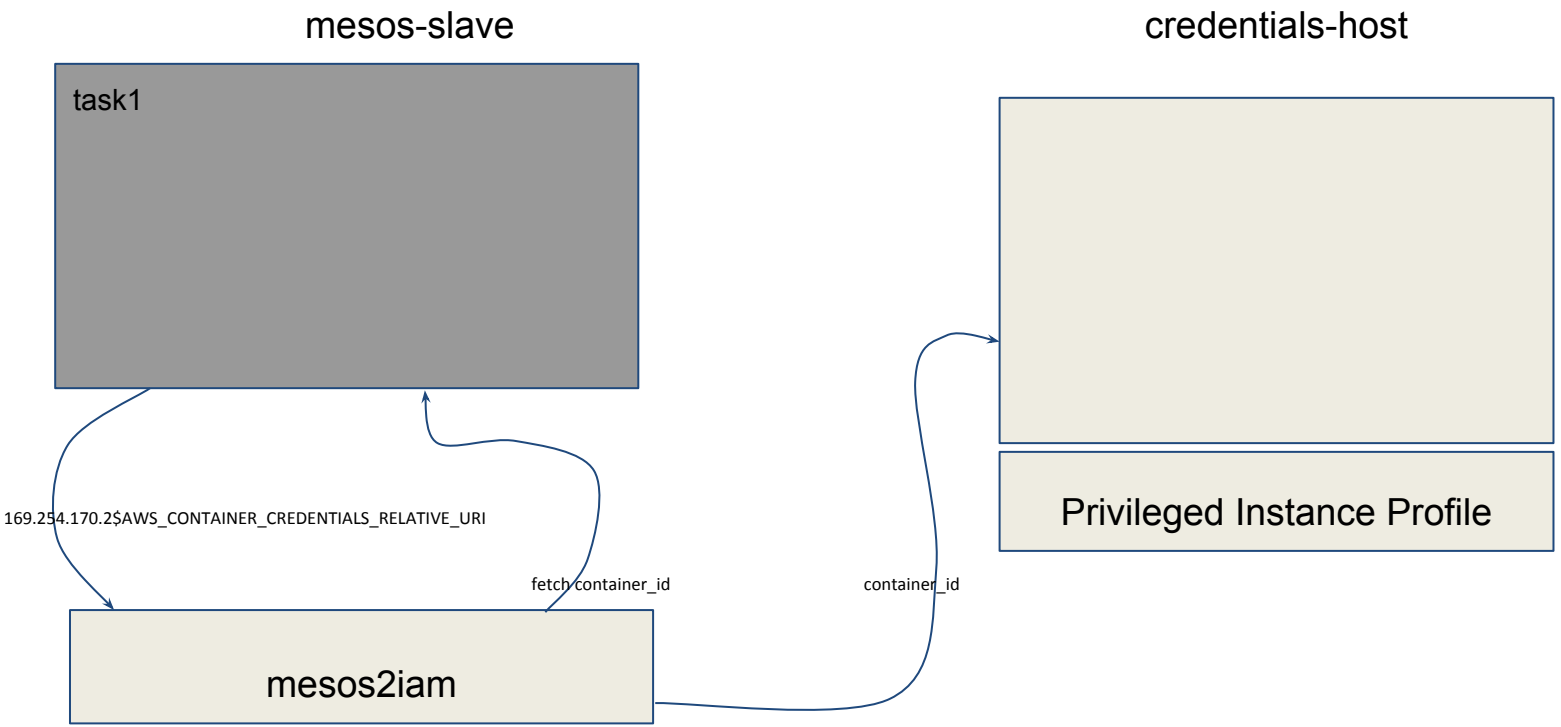
THE LINUX FOUNDATION

mesos2iam



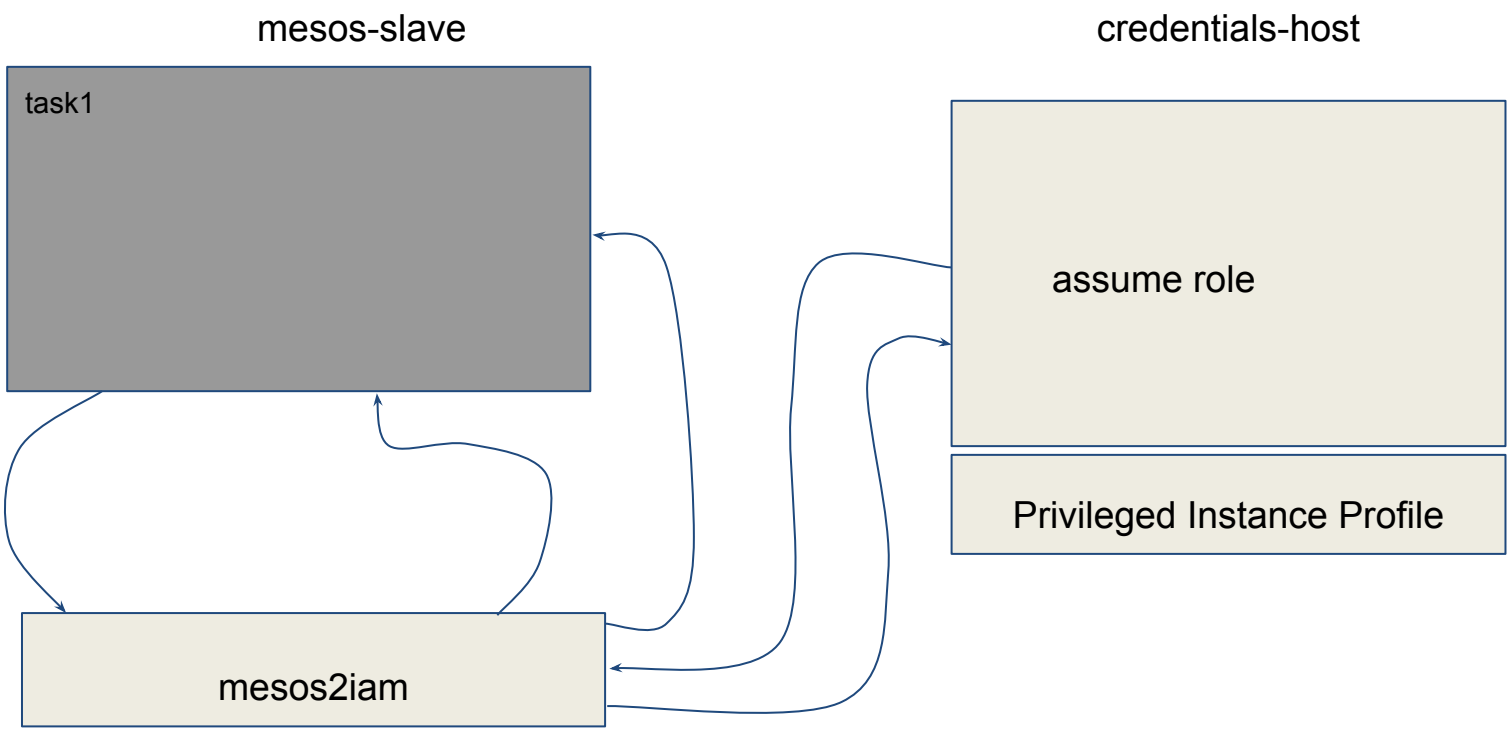
THE LINUX FOUNDATION

mesos2iam



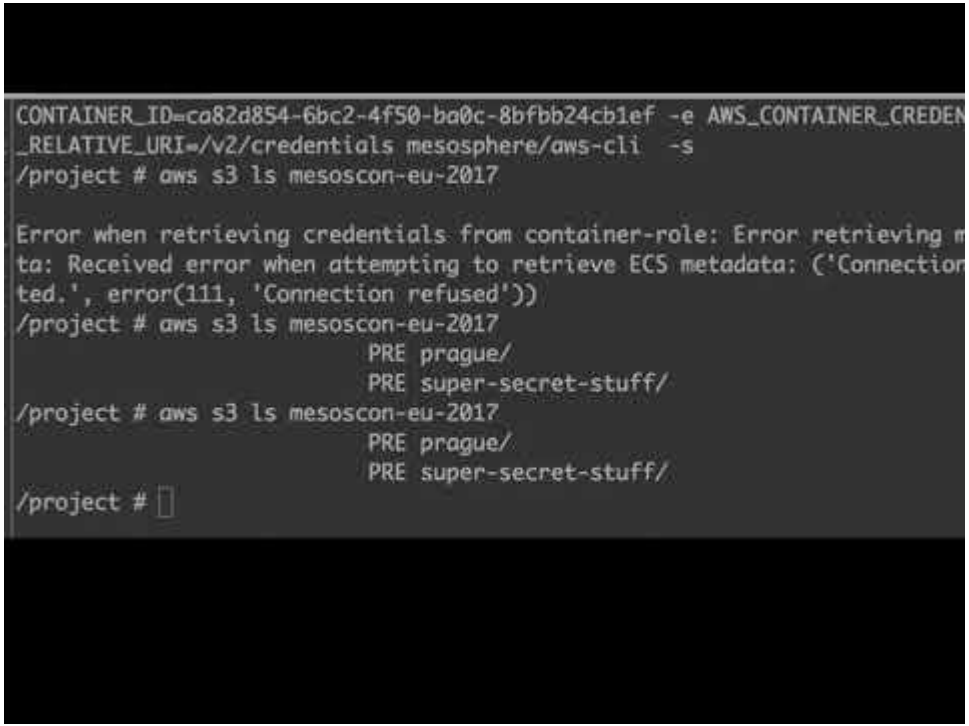
THE LINUX FOUNDATION

mesos2iam



THE LINUX FOUNDATION

demo time



https://www.youtube.com/watch?v=ra3SOeO_yp0

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

Opensource

CONTRIBUTIONS WELCOME

mesos2iam:https://github.com/schibsted/mesos2iam
smaug(naive credentials api):https://github.com/schibsted/smaug
deathnode: https://github.com/alanbover/deathnode

SCHIBSTED MEDIA GROUP

THE LINUX FOUNDATION

QUESTIONS?

MesosCon
EUROPE