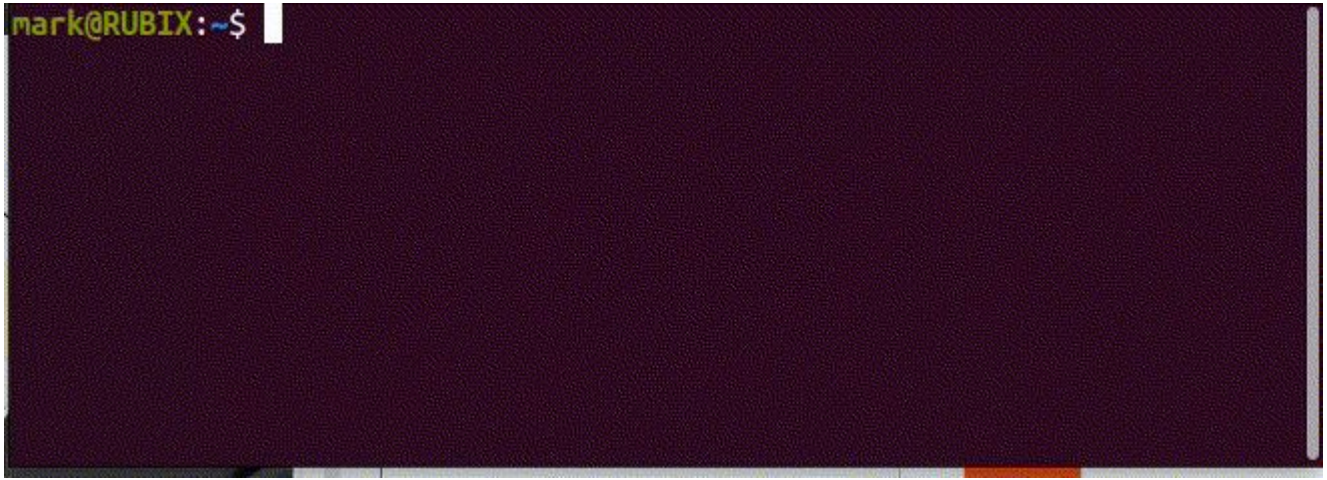
Access management in LXD

FOSDEM 2025

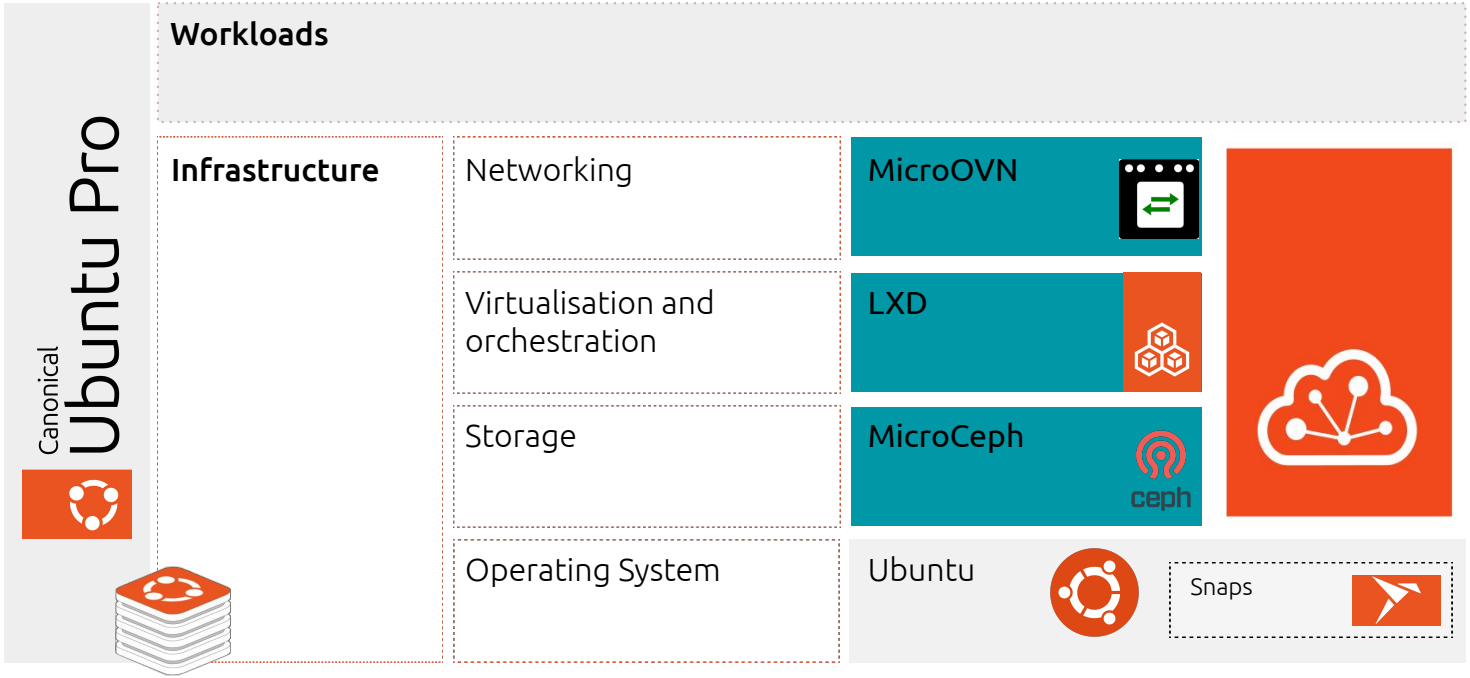
Mark Laing
Software Engineer (LXD)
Canonical

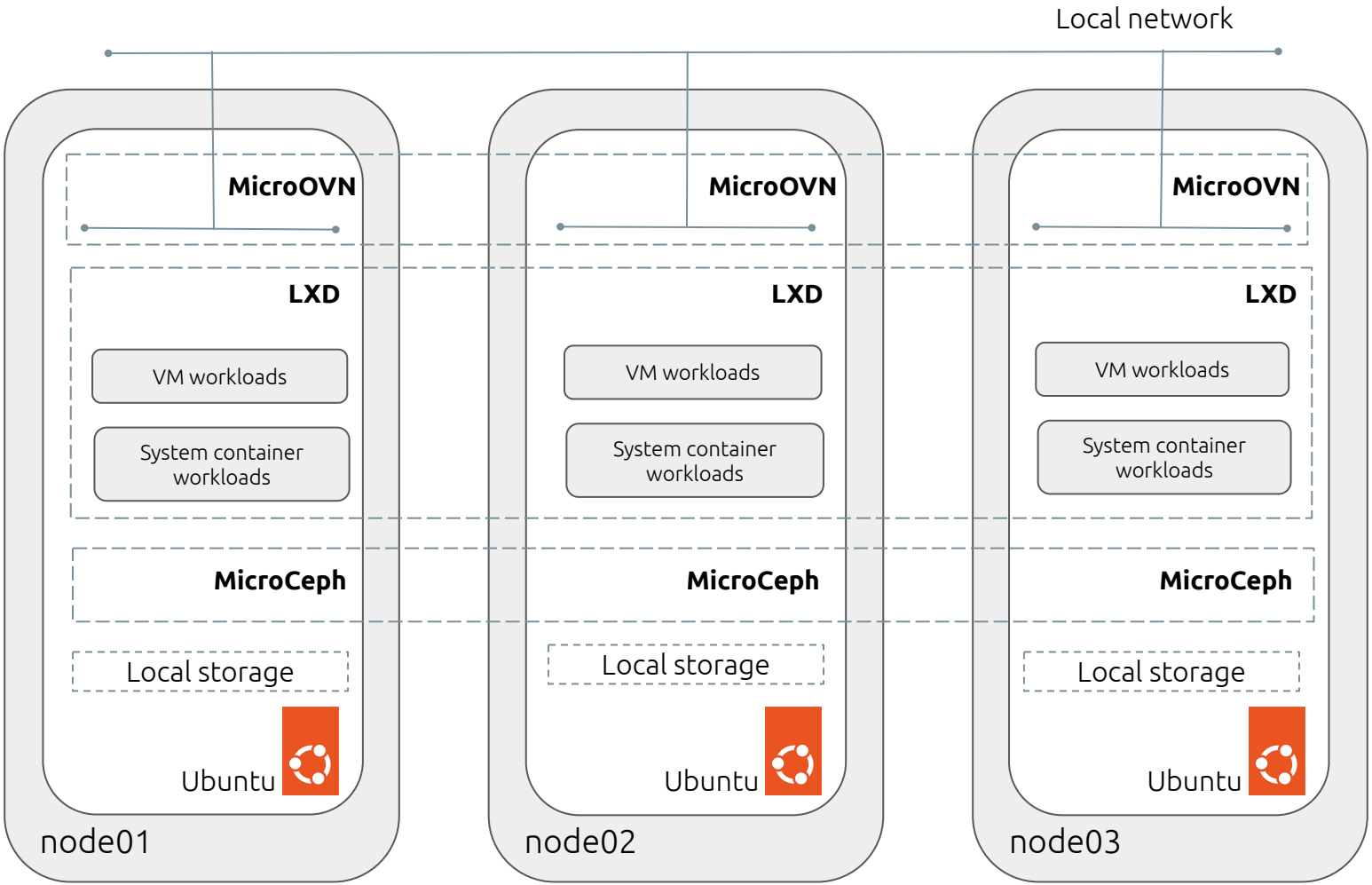
What is LXD?

LXD is a modern, secure and powerful system container and virtual machine manager.

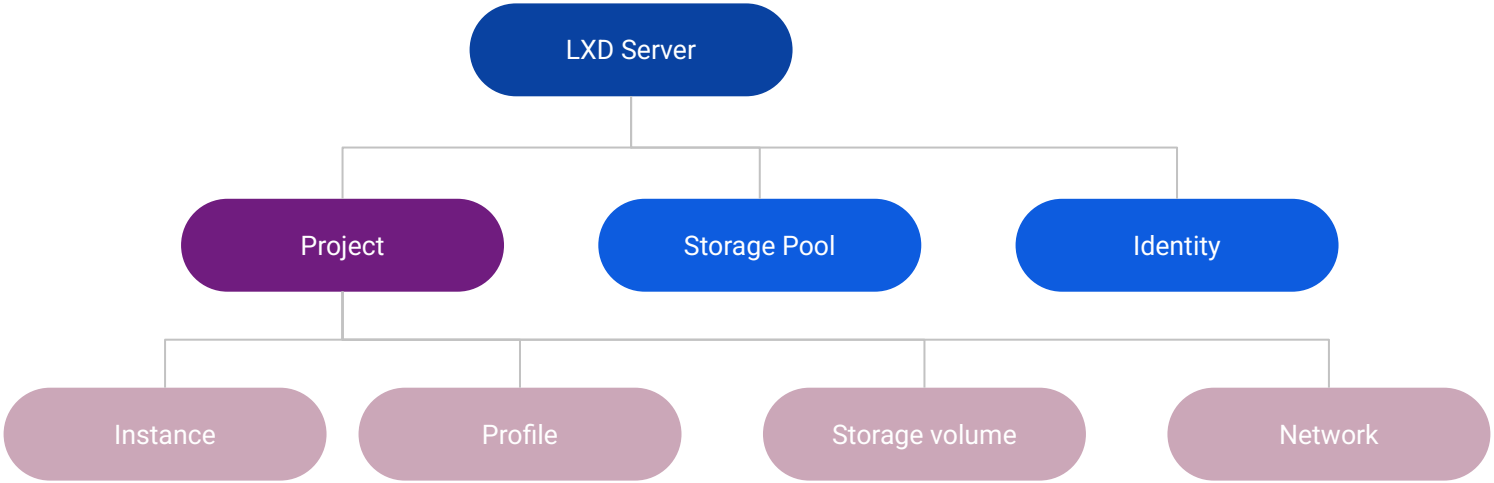


MicroCloud = LXD on rails




Local network
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node01
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node02
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node03

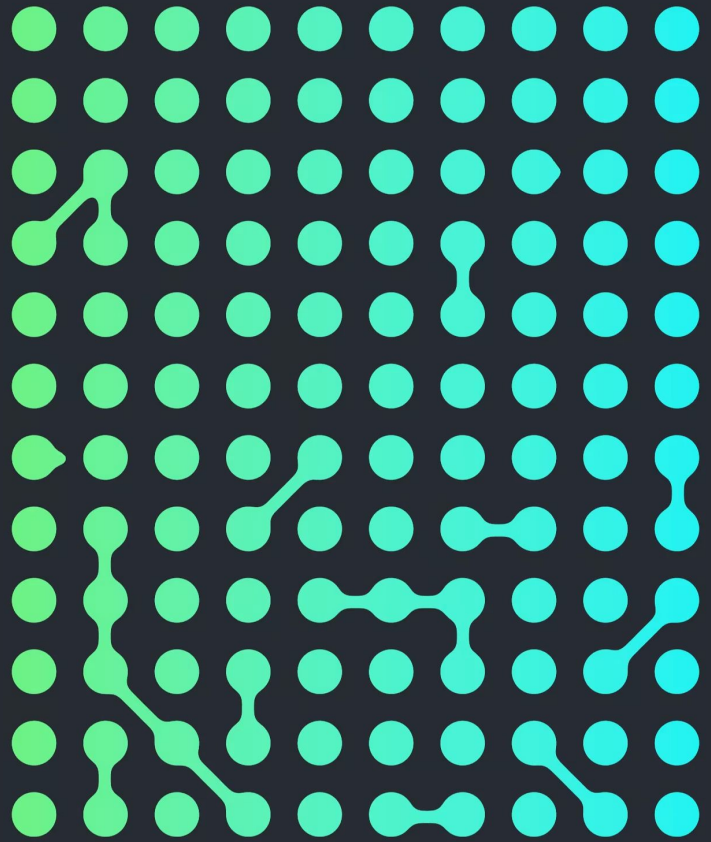
Existing authorization



OpenFGA™

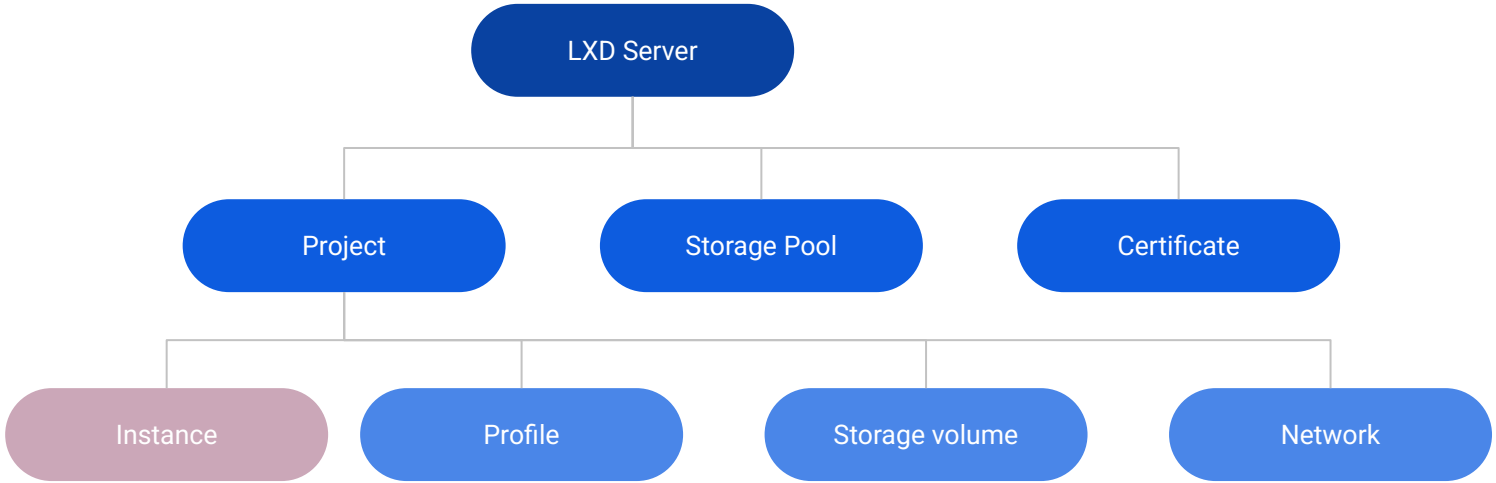
Relationship-based access control made fast, scalable, and easy to use.

OpenFGA is an open-source authorization solution that allows developers to build granular access control using an easy-to-read modeling language and friendly APIs.



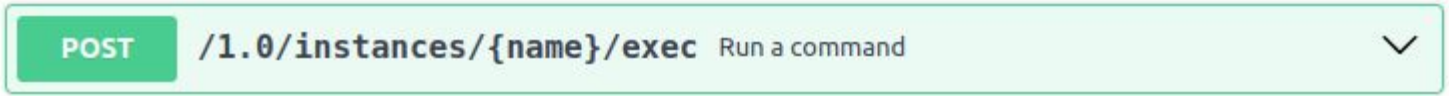
Fine-grained authorization

Does user `X` have relation `can_exec` with instance `c1`?



Fine-grained authorization

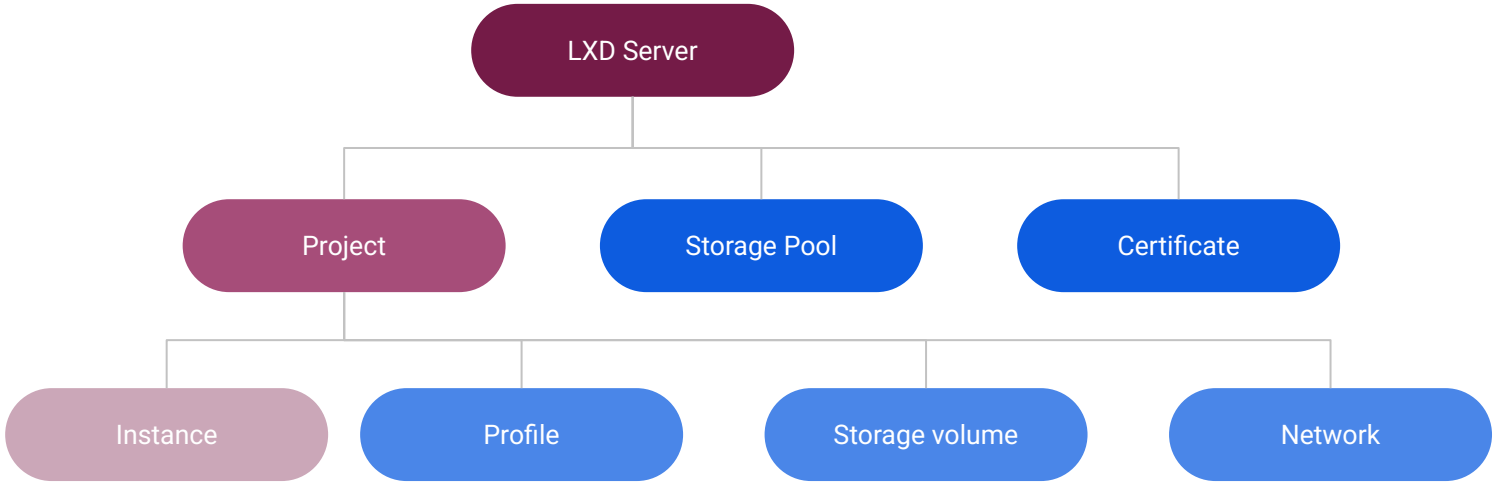
Does user `X` have relation `can_exec` with instance `c1`?




```
type identity
type instance
  relations
    can_exec: [identity]
```

Fine-grained authorization

Does user `X` have relation `can_exec` with instance `c1`?



Fine-grained authorization

POST /1.0/instances/{name}/exec Run a command

```
type identity
type server
  relations
    admin: [identity]
type project
  relations
    server: [server]
    operator: [identity] or admin from server
    can_operate_instances: [identity] or operator
type instance
  relations
    project: [project]
    can_exec: [identity] or can_operate_instances from project
```

Computed relation.

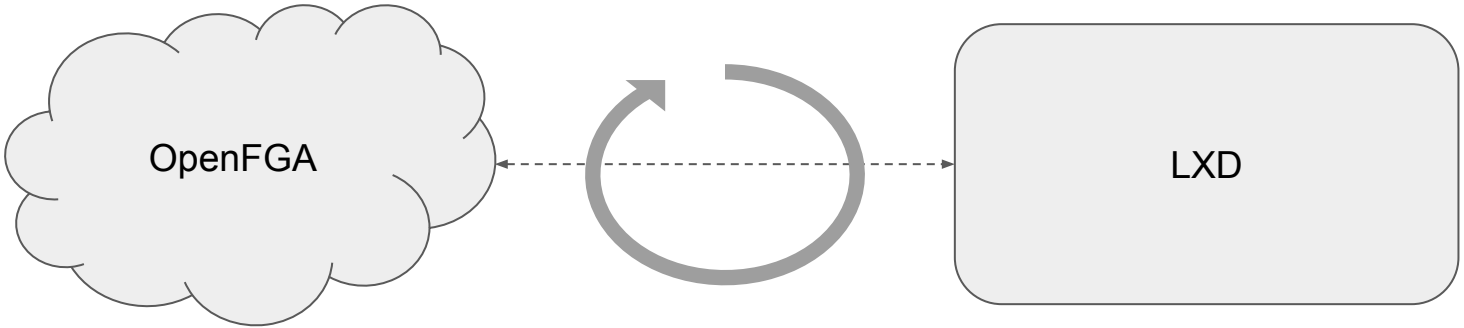
Computed relation.

Tuples, tuples, tuples…

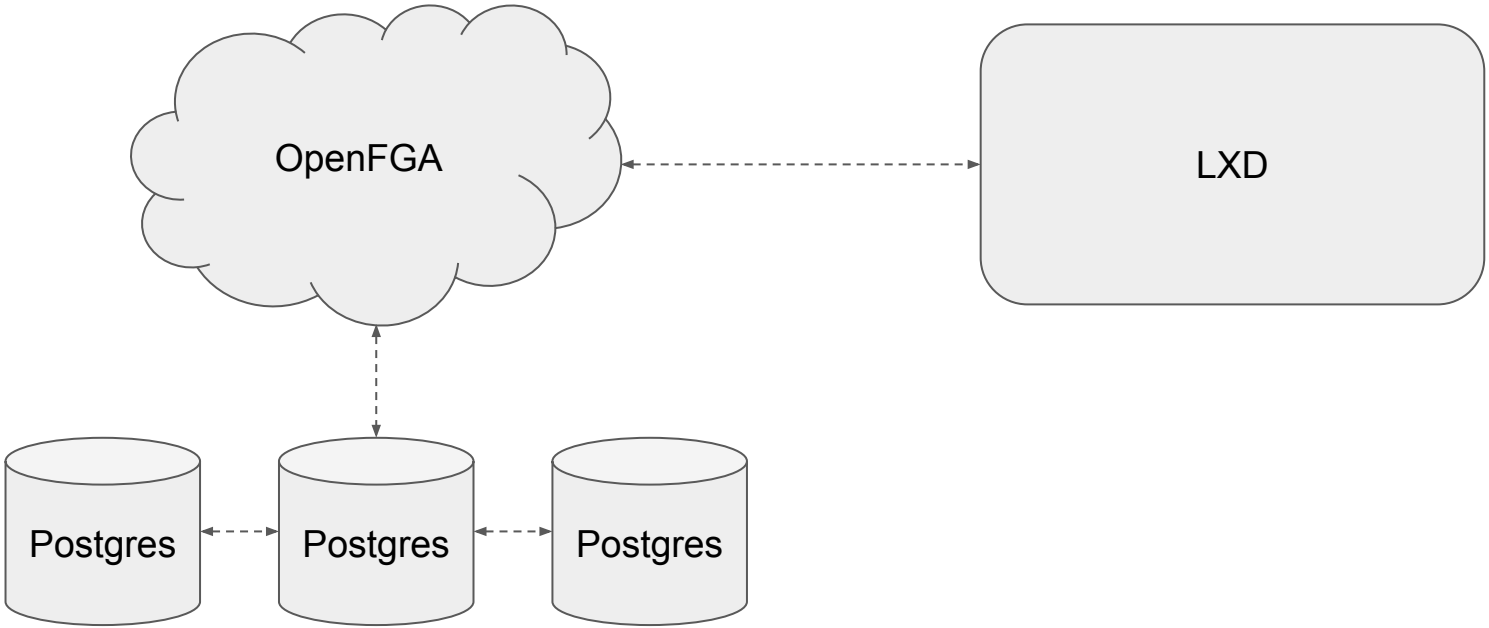
```
# User is related to project via `operator` if they are related to
# server via `admin`.
USER server:/1.0
RELATION server
OBJECT project:/1.0/projects/default

# User has `can_exec` on instance if they have `operator` or
#`can_operate_instances` on project.
USER project:/1.0/projects/default
RELATION project
OBJECT instance:/1.0/instances/c1?project=default
```

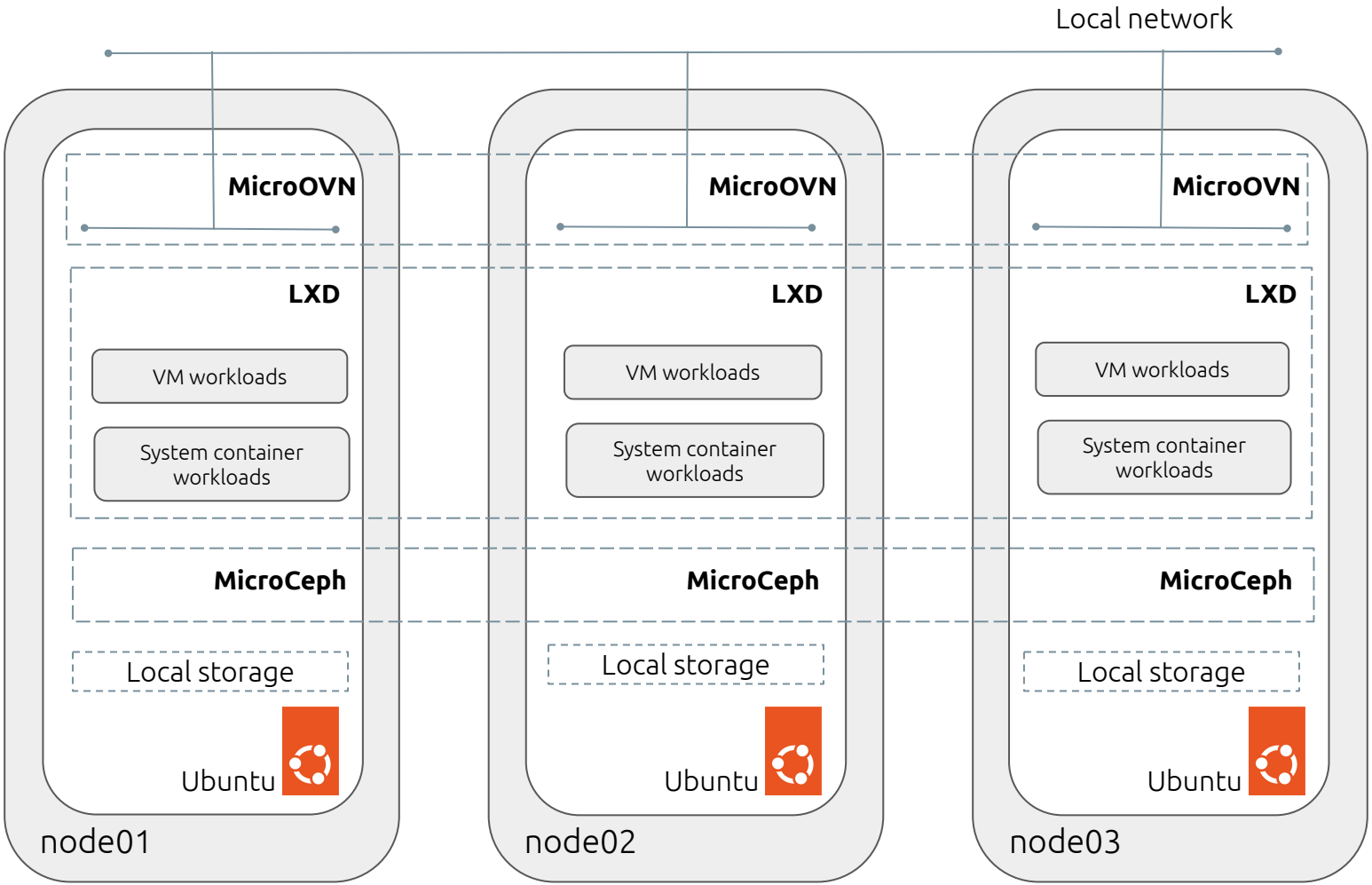
External OpenFGA

Does user `X` have relation `can_exec` with instance `c1`?

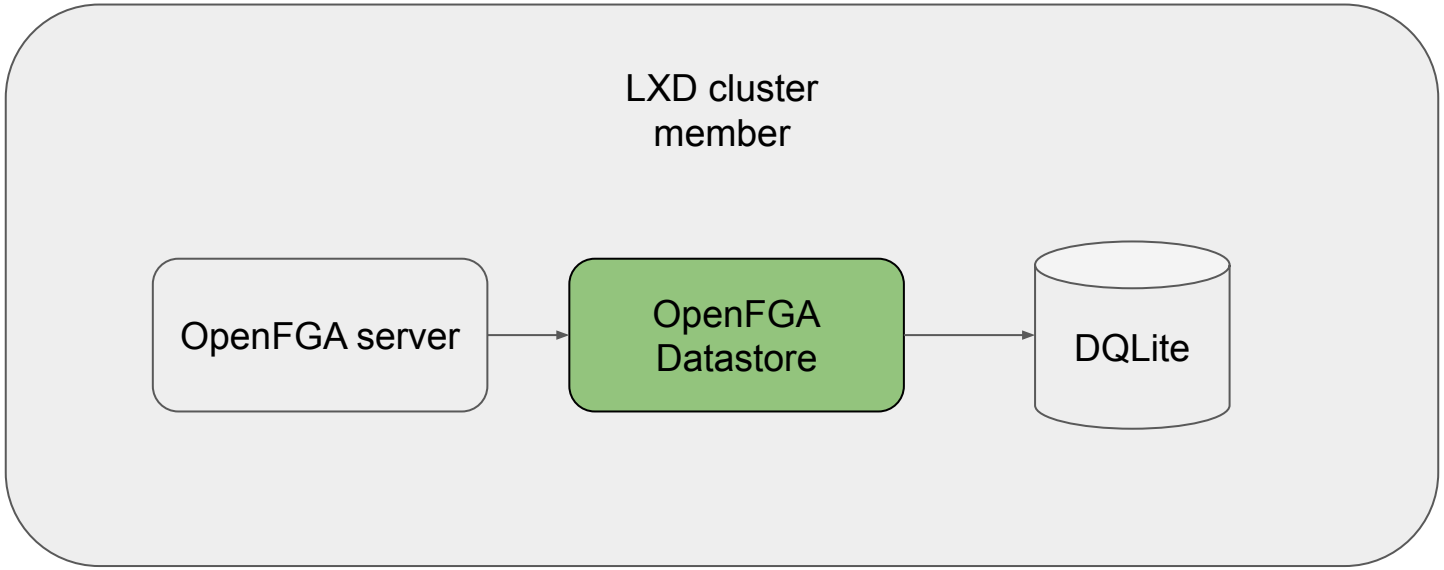


External OpenFGA




Local network
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node01
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node02
MicroOVN
LXD
VM workloads
System container workloads
MicroCeph
Local storage
Ubuntu
node03

Embedded OpenFGA



OpenFGA Datastore

`ReadUsersetTuples` List all tuples where the “user” is a given type, that are related to a given object, by a given relation*.

```
USER identity:{expand this part}
RELATION can_view
OBJECT project:/1.0/projects/default
```

`ReadStartingFromUser` List all tuples that are related to a given user*.

```
USER identity:/1.0/auth/identities/tls/{fingerprint}
RELATION {filter on this or expand if not given}
OBJECT {expand this part}
```

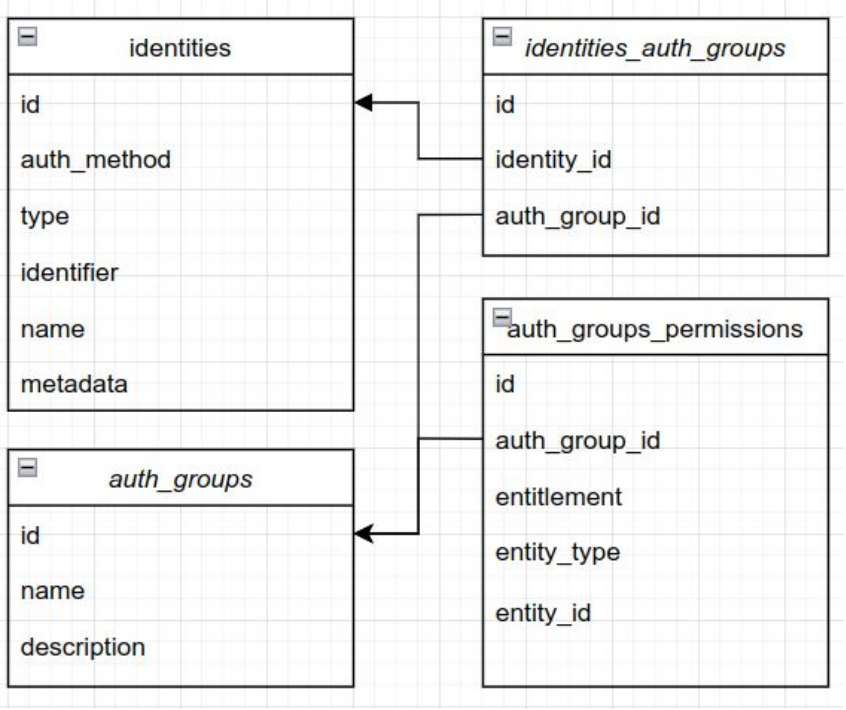
** Not 100% accurate…*

OpenFGA Datastore

Does user `/1.0/auth/identities/tls/{fingerprint}` **have relation** `can_exec` **with instance** `/1.0/instances/c1?project=default`**?**

POST `/1.0/instances/{name}/exec` Run a command

1. Which groups does the identity belong to? *Contextual tuples.*
2. What permissions do members of these groups have? *Cached per request.*



Demo time!

Pros and cons

Pros	Cons
• Works out-of-the-box • OpenFGA + Postgres deployment not necessary! • Cluster database is source of truth. • Easier model migrations.	• Complexity. • Stored user information (GDPR). • OpenFGADatastore interface updates. • Further optimisation required.

Thank you listening! Questions?

Microcloud

OpenFGA

Mark Laing
mark.laing@canonical.com