Authorization: Ensuring Only Ada Can Access Her Files

Joy Ebertz
Sr Staff Software Engineer
@Split

DEVOPS WORLD by CloudBees

Agenda

- What is Authorization?
- Levels of Authorization
- Types of Access Control
- Typical Architecture

What is Authorization?

And Other Definitions

Authentication vs Authorization

Authentication (AuthN)

The process or action of verifying the identity of a user or process.

Authentication vs Authorization

Authorization (AuthZ)

The function of specifying access rights/privileges to resources. (i.e. defining the access policies)

Authentication vs Authorization

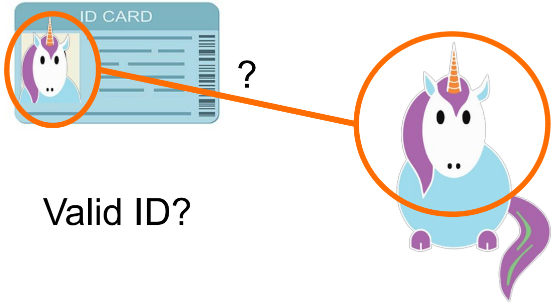
Authentication (AuthN)

Authentication vs Authorization

Valid ID?

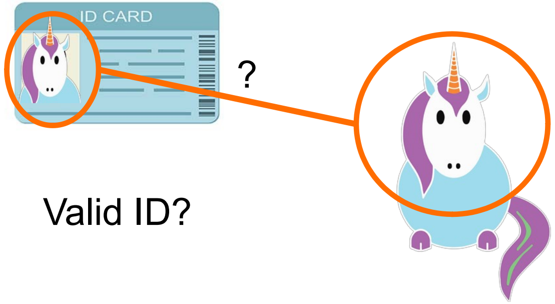
Authentication (AuthN)

Authentication vs Authorization



Authentication (AuthN)

Authentication vs Authorization

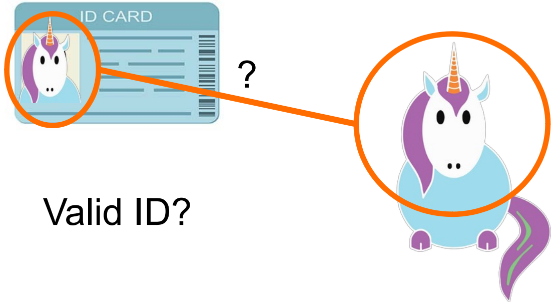


Valid ID?

Authentication (AuthN)

Authorization (AuthZ)

Authentication vs Authorization



Authentication (AuthN)

Authorization (AuthZ)

is 21?
ID CARD

Authentication vs Authorization

Access Control

The restriction of Access

Authorization

Authentication vs Authorization

Access Management

*The **process** of restricting of Access*

Authorization

Authentication vs Authorization

Identity and Access Management (IAM)

The framework of policies and technologies encompassing authentication and authorization.

Also called Identity Management (IdM)

Authorization

Authentication vs Authorization

AWS Identity and Access Management (AWS IAM)

AWS's customer-facing authorization management feature.

Authorization

Authentication vs Authorization

Authorization (AuthZ)

Access Control
Access Management
Permissions

Levels of Authorization

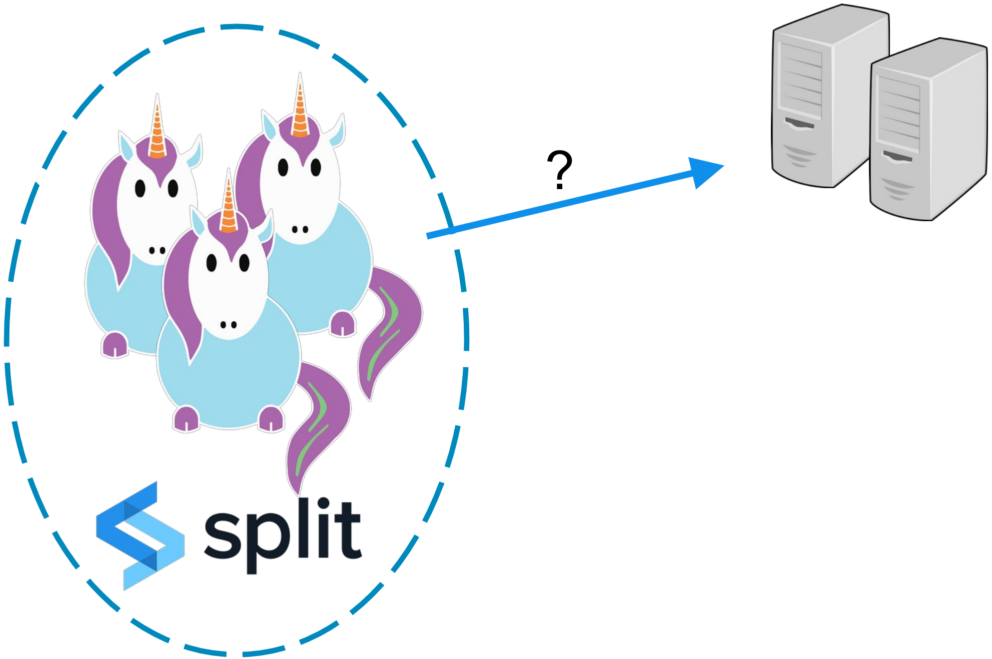
DEVOPS WORLD by CloudBees

Levels of Authorization

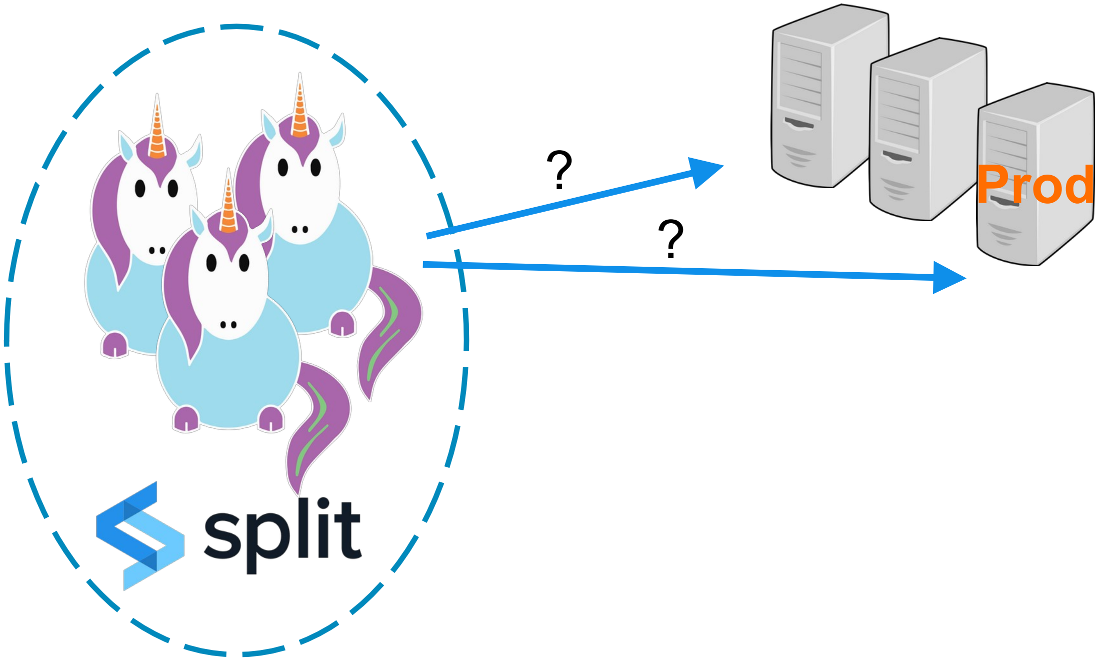
- System and Infrastructure Authorization
- Customer-Facing Authorization Feature
- Application Level Authorization

System and Infrastructure Authorization

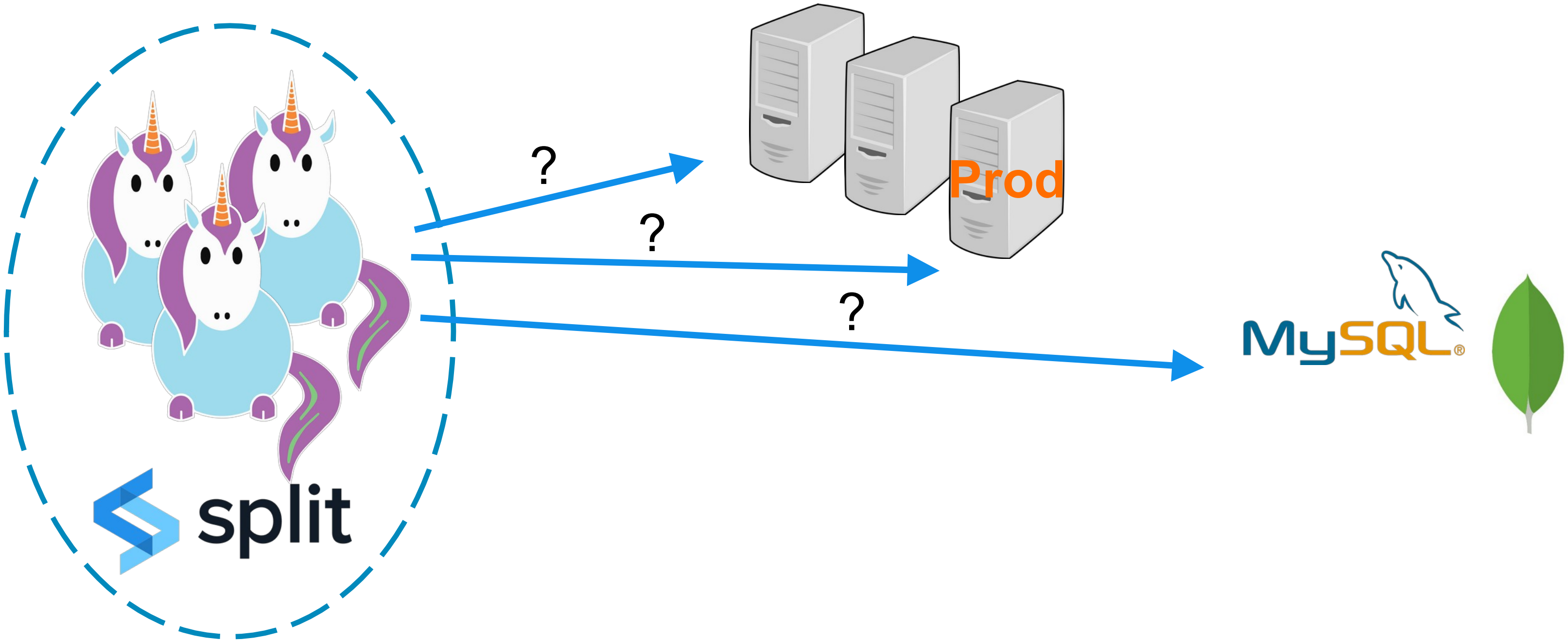
System and Infrastructure Authorization



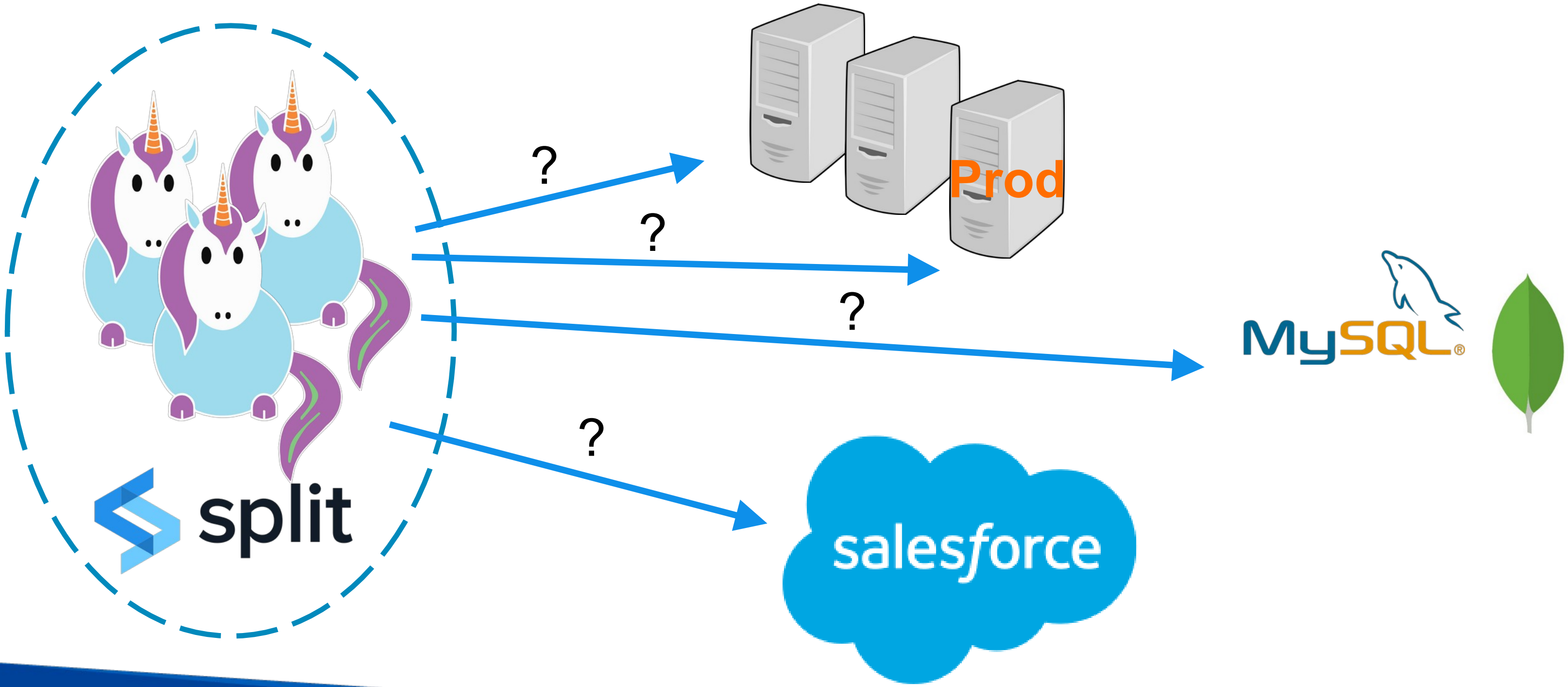
System and Infrastructure Authorization



System and Infrastructure Authorization



System and Infrastructure Authorization



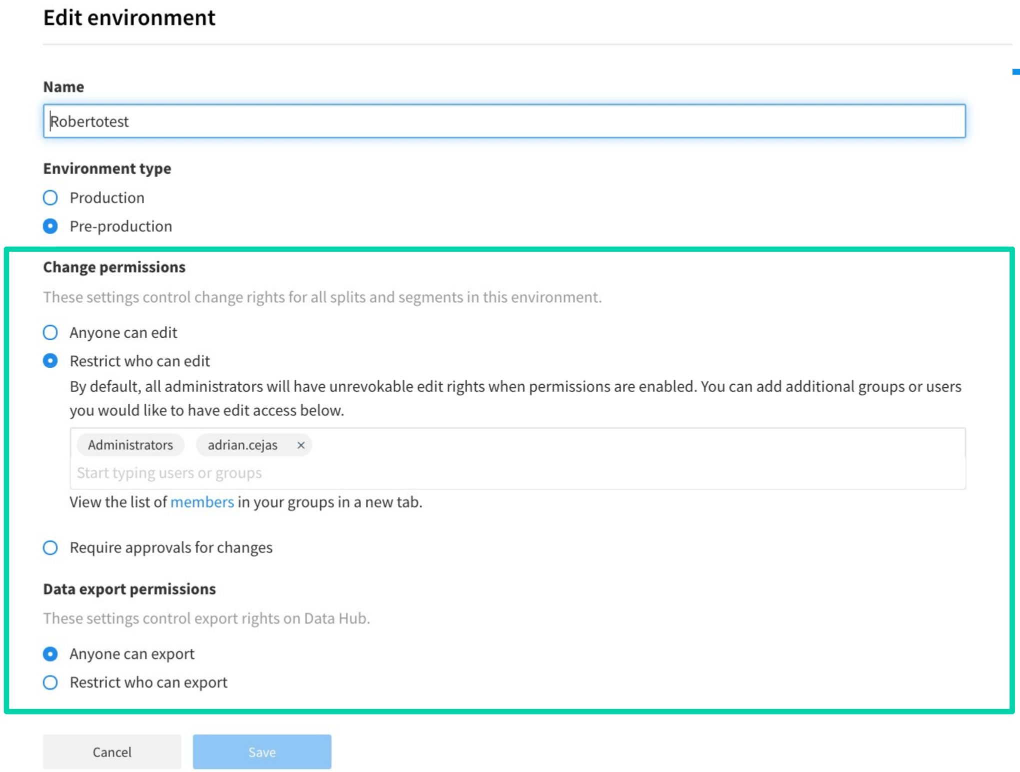
System and Infrastructure Authorization

okta

Auth0

Active Directory

Customer-Facing Feature



Edit environment

Name

Robertotest

Environment type

○ Production

● Pre-production

Change permissions

These settings control change rights for all splits and segments in this environment.

○ Anyone can edit

● Restrict who can edit

By default, all administrators will have unrevokable edit rights when permissions are enabled. You can add additional groups or users you would like to have edit access below.

Administrators | adrian.cejas ×

Start typing users or groups

View the list of members in your groups in a new tab.

○ Require approvals for changes

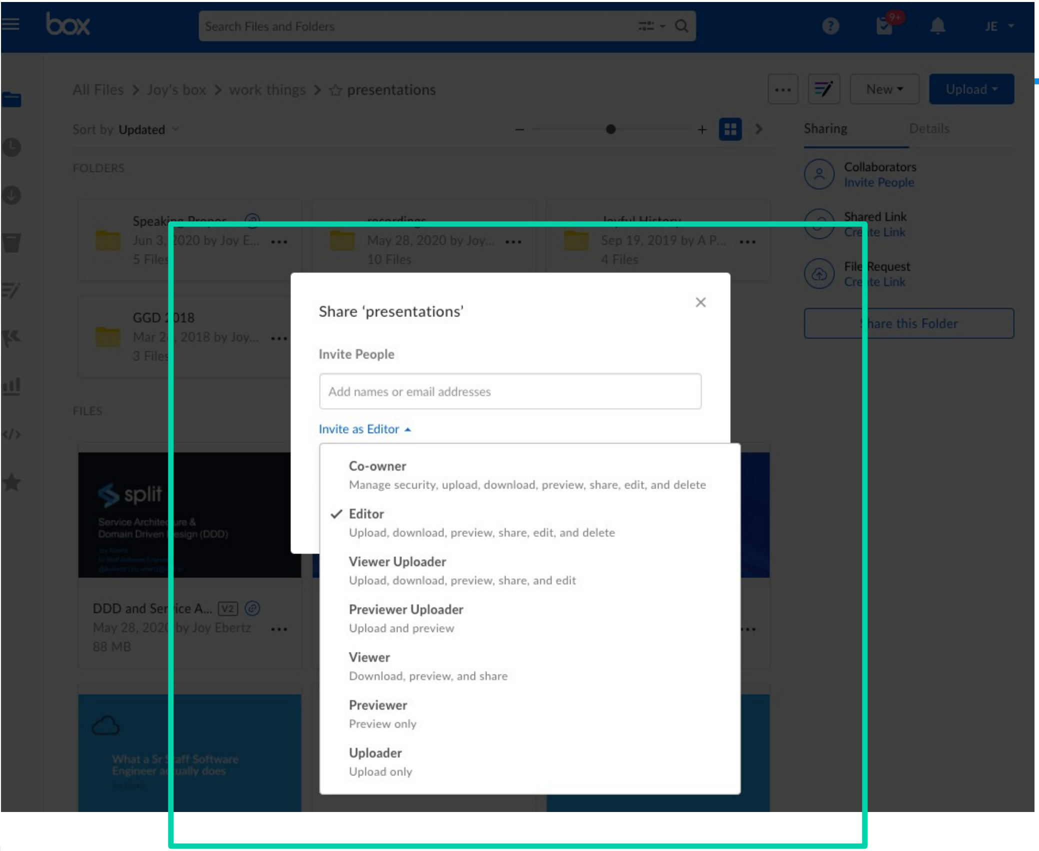
Data export permissions

These settings control export rights on Data Hub.

● Anyone can export

○ Restrict who can export

Customer-Facing Feature



Share 'presentations'

Invite People

Add names or email addresses

Invite as Editor

Co-owner
Manage security, upload, download, preview, share, edit, and delete

✓ **Editor**
Upload, download, preview, share, edit, and delete

Viewer Uploader
Upload, download, preview, share, and edit

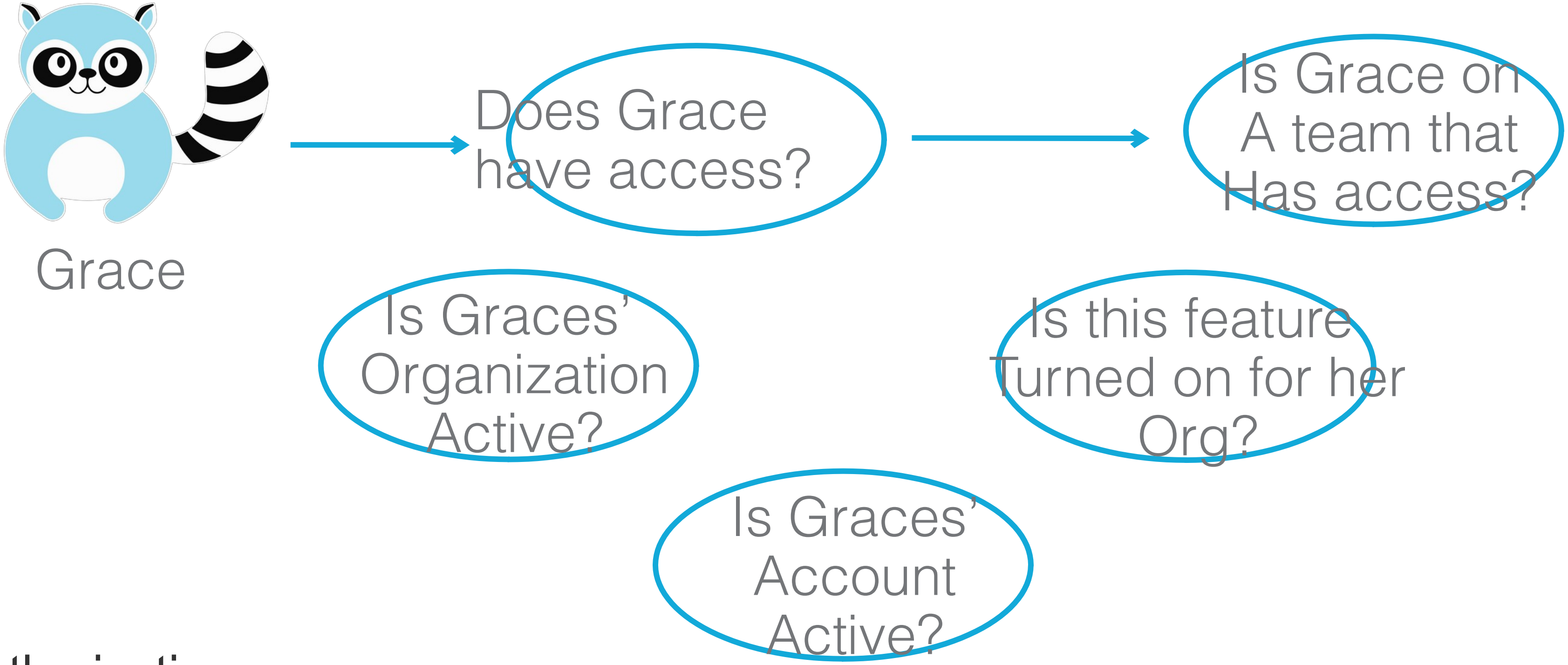
Previewer Uploader
Upload and preview

Viewer
Download, preview, and share

Previewer
Preview only

Uploader
Upload only

Application Level Authorization



Grace

Does Grace have access?

Is Grace on A team that Has access?

Is Graces' Organization Active?

Is this feature Turned on for her Org?

Is Graces' Account Active?

Levels of Authorization

- System and Infrastructure Authorization
- Customer-Facing Authorization Feature
- Application Level Authorization

Types of Access Control

DEVOPS WORLD by CloudBees

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Who controls access and/or policies?

Types of Access Control

Mandatory Access Control

MAC Is an operating system level access control where the policies are controlled by a central policy administrator and users cannot override policies.

Types of Access Control

Discretionary Access Control

DAC allows users in the system to grant access to objects. In many implementations, objects in the system have an owner and owners control access to those objects.*

**However, the formal definition doesn't say anything about owners*

Types of Access Control: MAC & DAC

Grace

Types of Access Control: MAC & DAC

Grace

Ada

Katherin
e

Types of Access Control: MAC & DAC

Grace

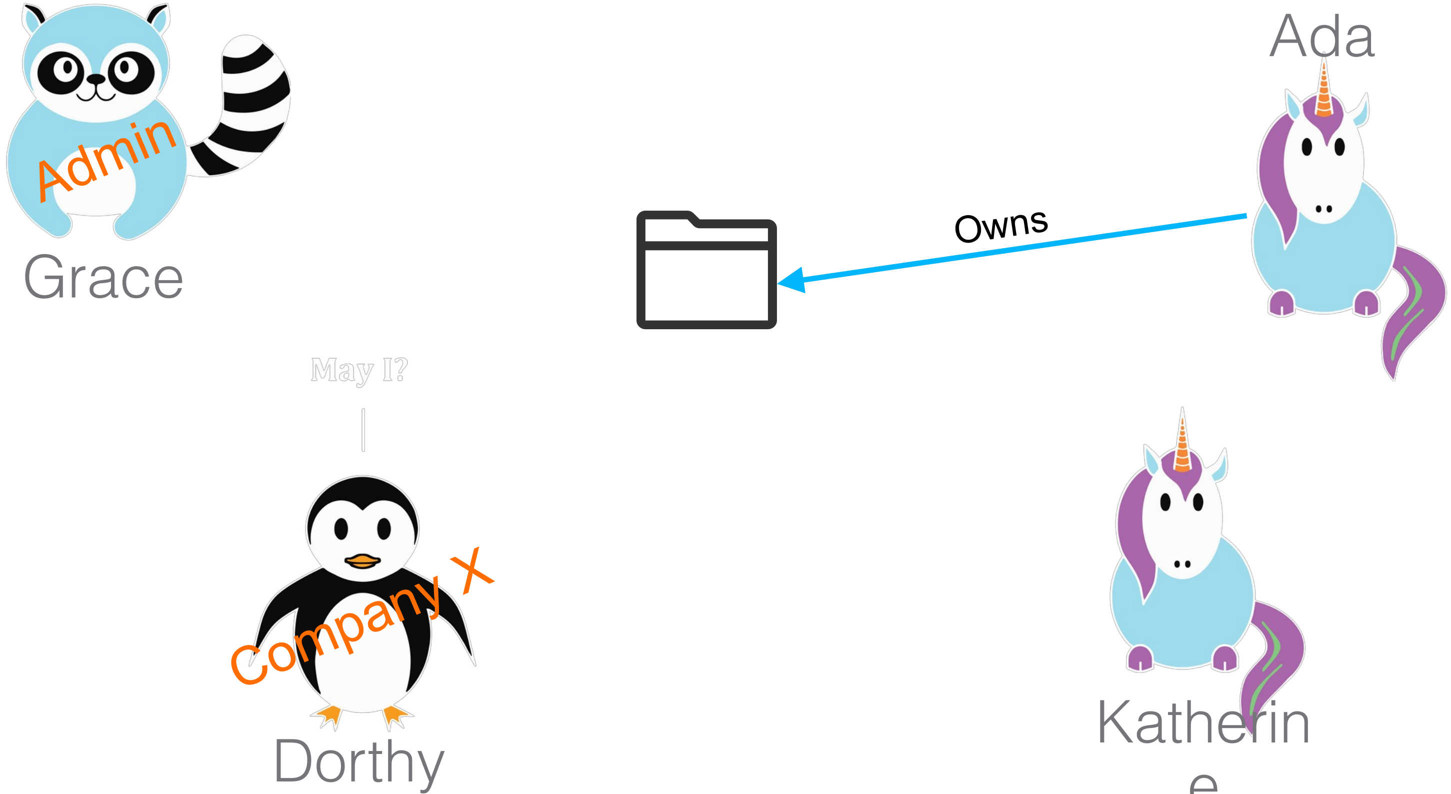
Ada

May I?

Dorthy

Katherin
e

Types of Access Control: MAC & DAC



Admin

Grace

Ada

Owns

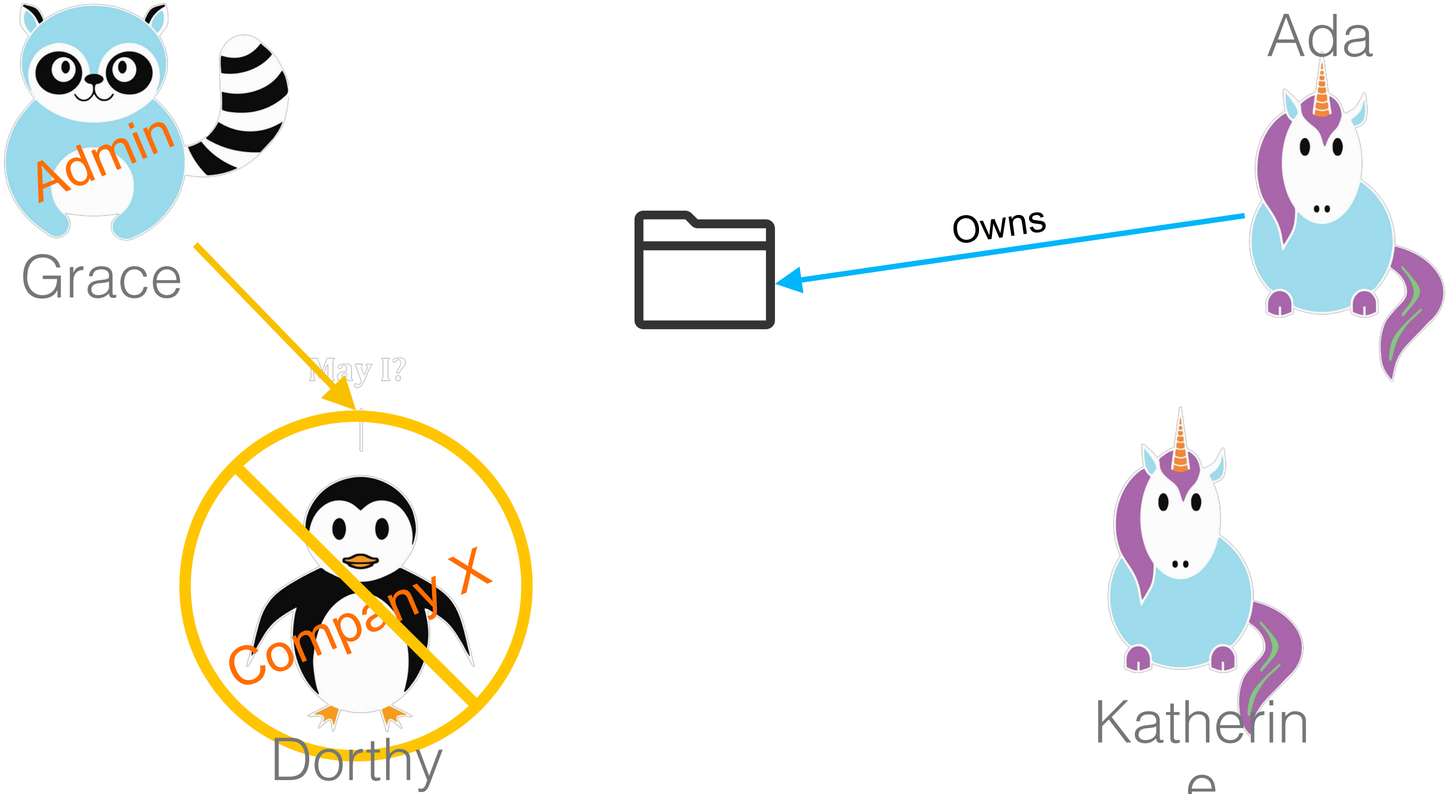
May I?

Company X

Dorthy

Katherin
e

Types of Access Control: MAC & DAC



Admin

Grace

May I?

Company X

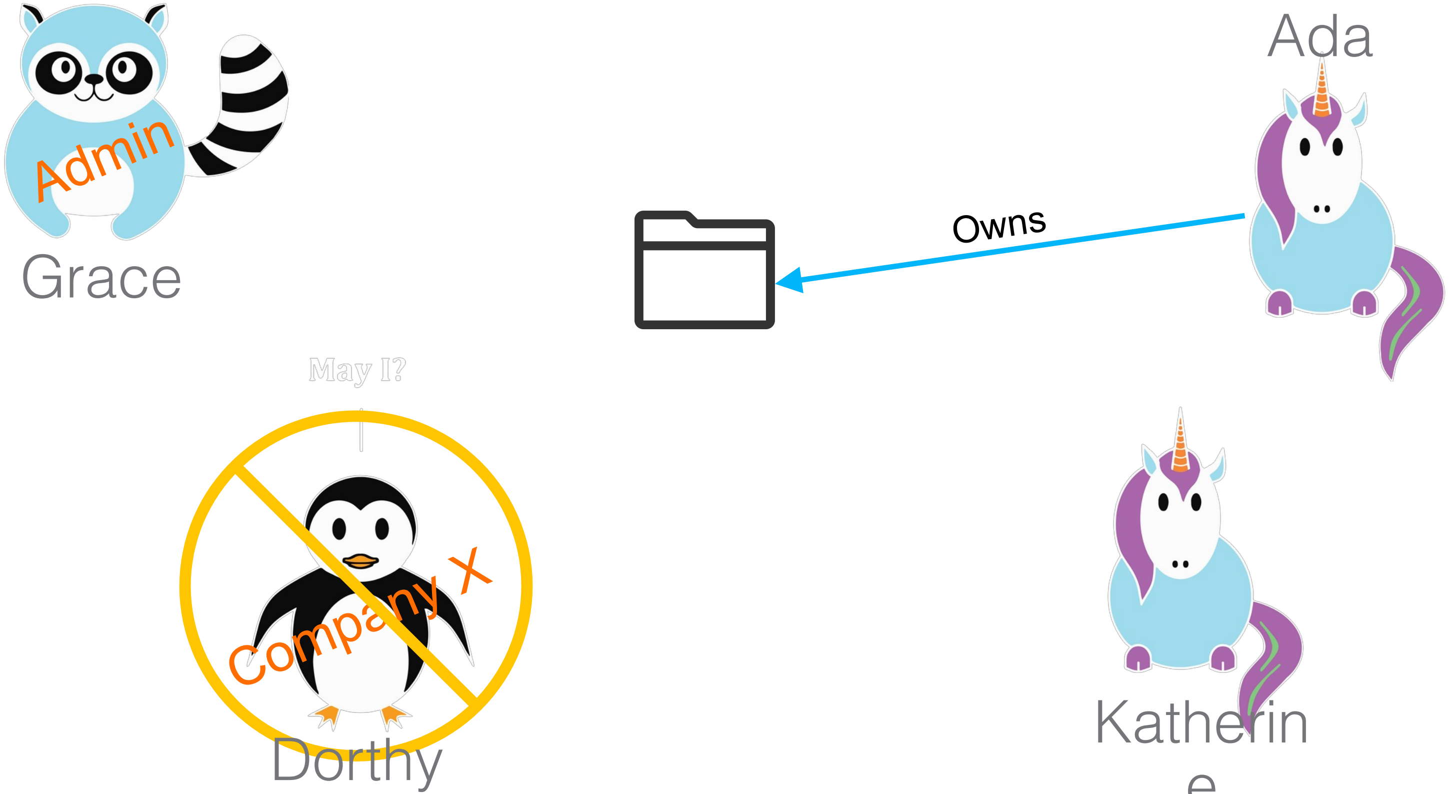
Dorthy

Owns

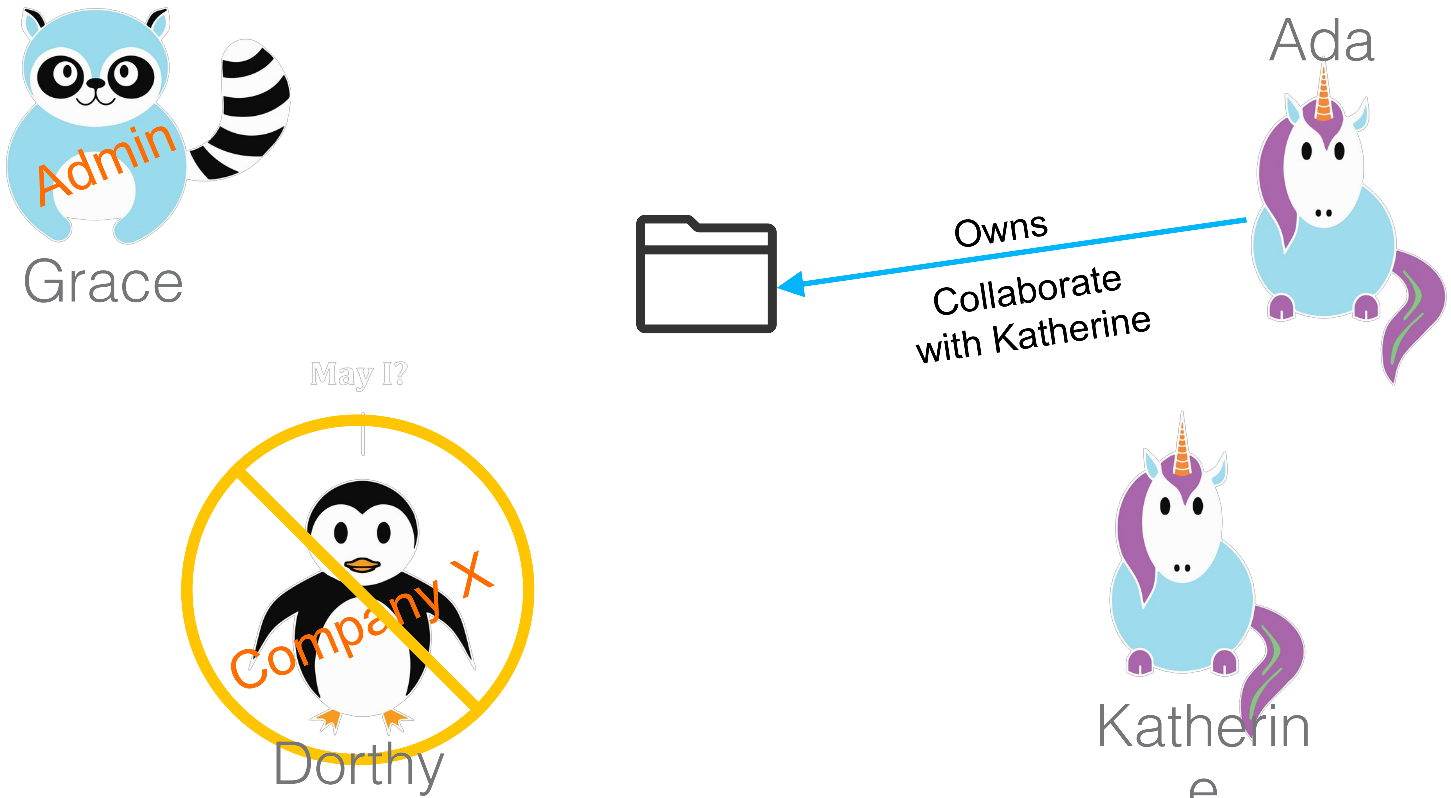
Ada

Katherine

Types of Access Control: MAC & DAC



Types of Access Control: MAC & DAC



Admin

Grace

Ada

Owns

Collaborate with Katherine

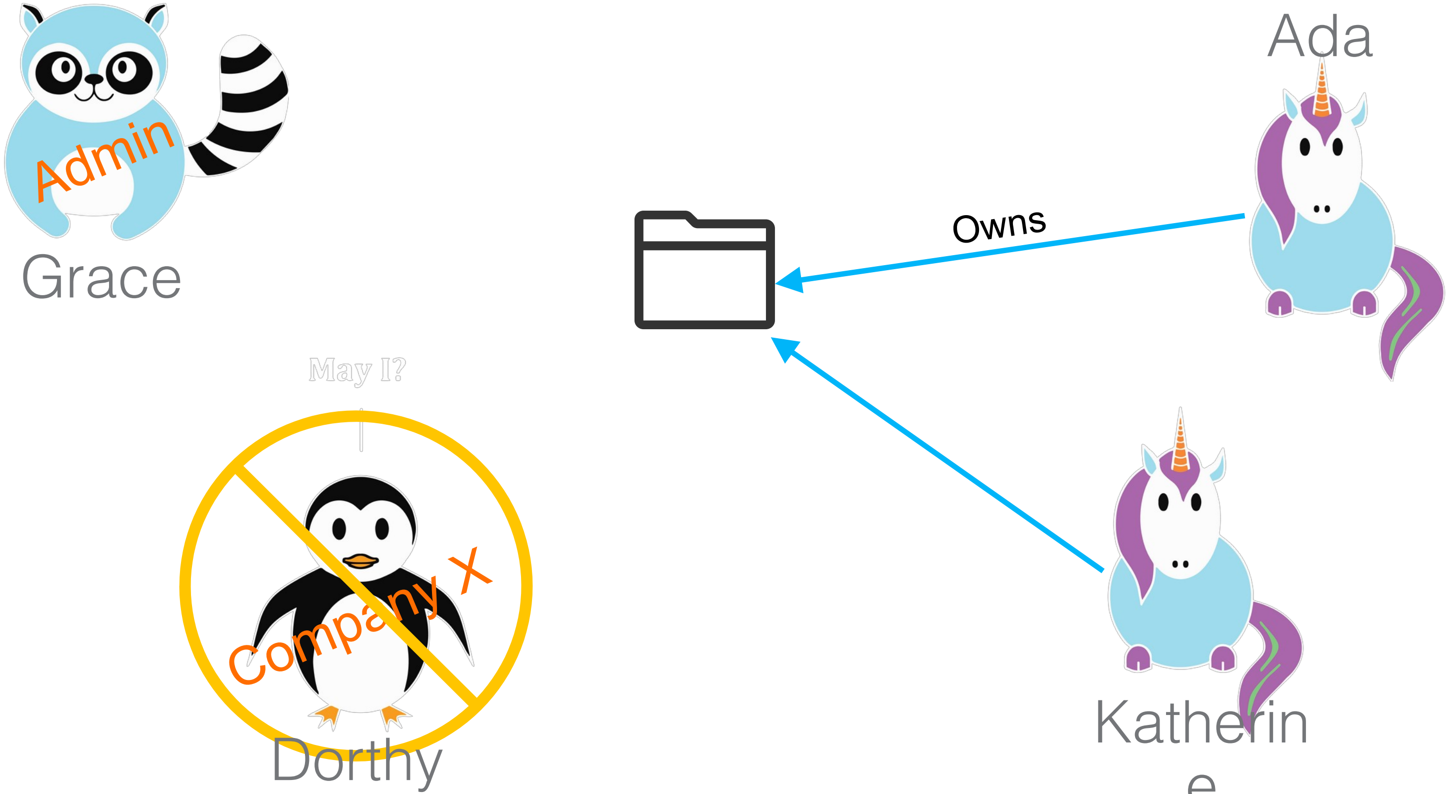
May I?

Company X

Dorthy

Katherin
e

Types of Access Control: MAC & DAC



split

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

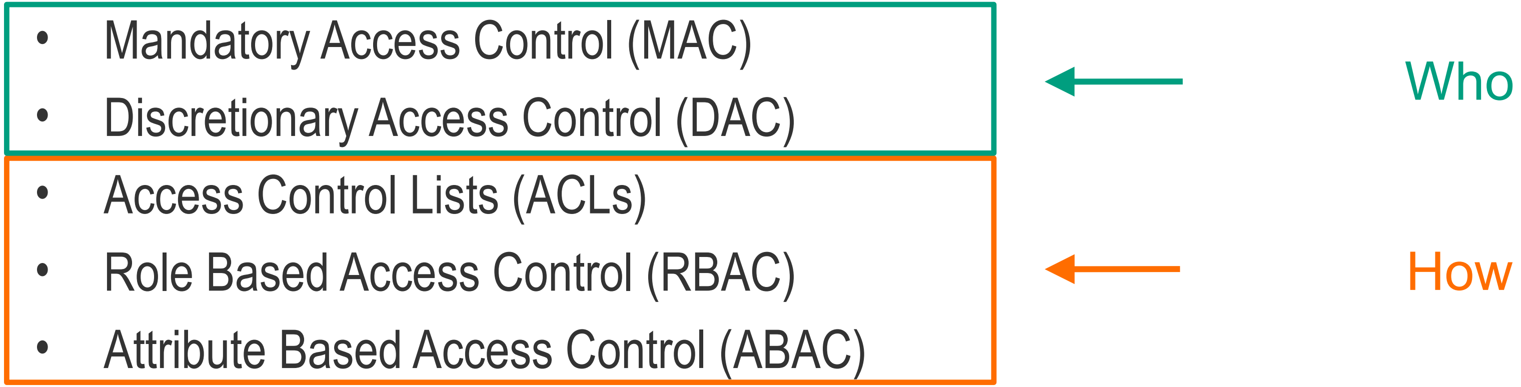
Who controls access and/or policies?

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

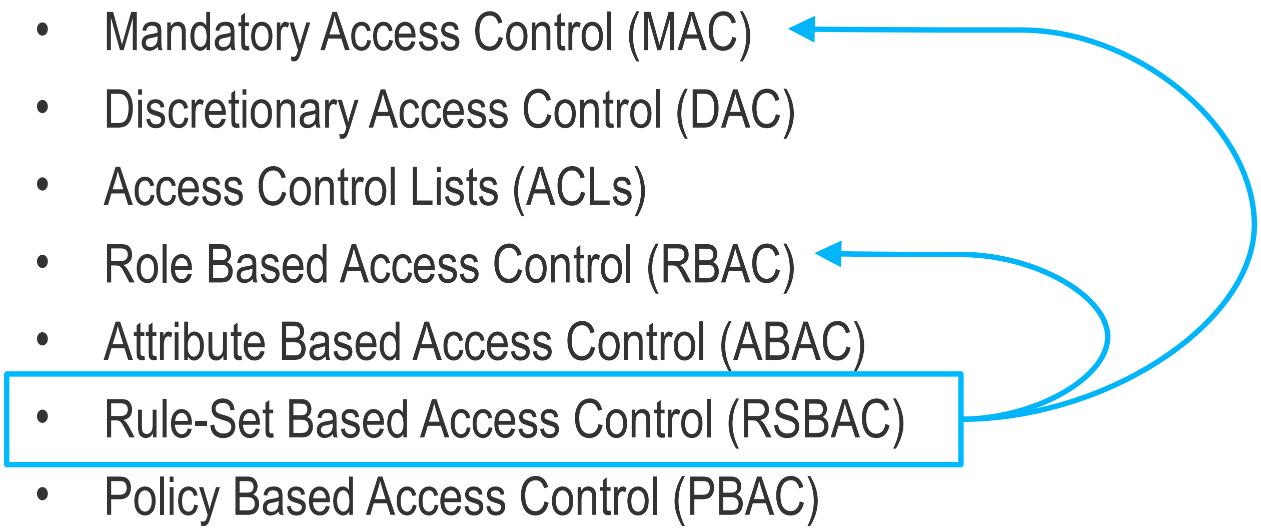
← How are the policies modeled?

Types of Access Control



- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Types of Access Control



- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- Policy Based Access Control (PBAC)

Types of Access Control

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- ~~Policy Based Access Control (PBAC)~~

Types of Access Control

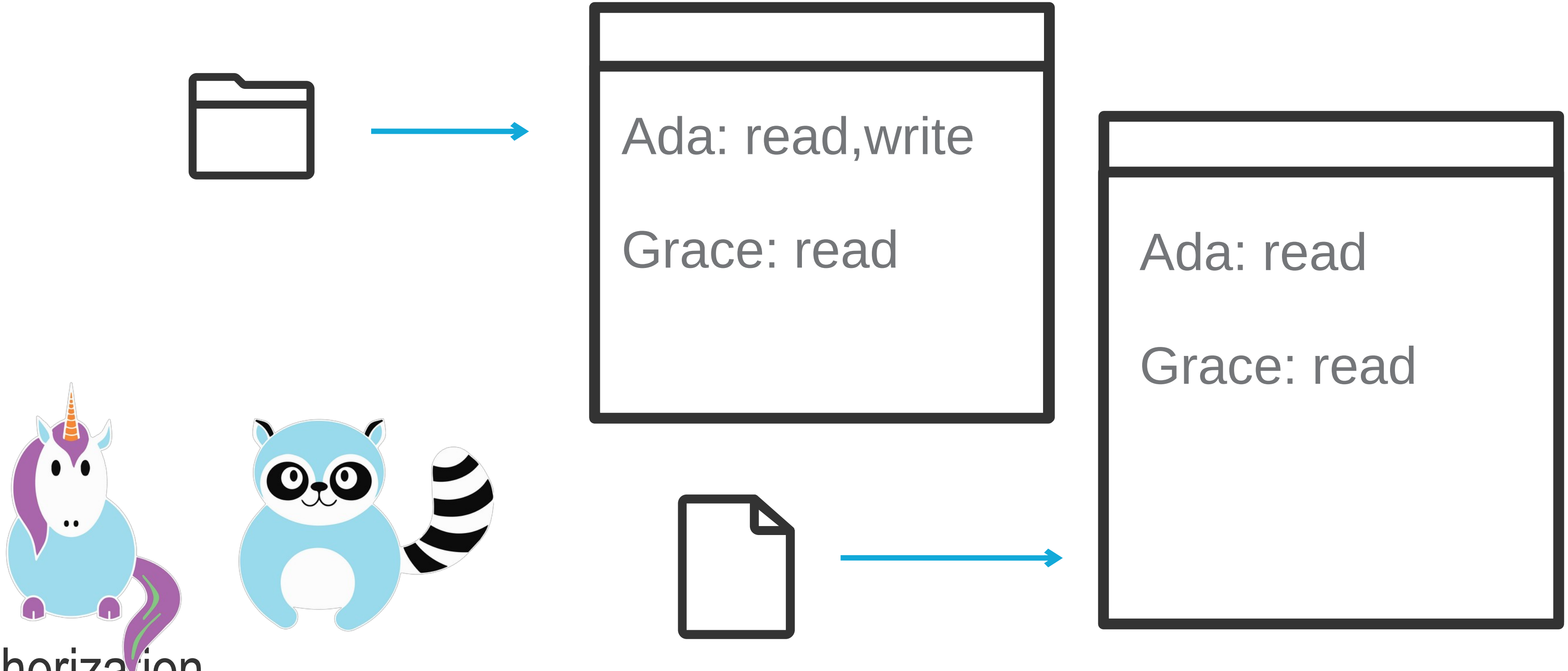
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Access Control Lists (ACLs)
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)
- Rule-Set Based Access Control (RSBAC)
- ~~Policy Based Access Control (PBAC)~~

How are the policies modeled?

Types of Access Control

ACLs

ACLs (Access Control Lists)



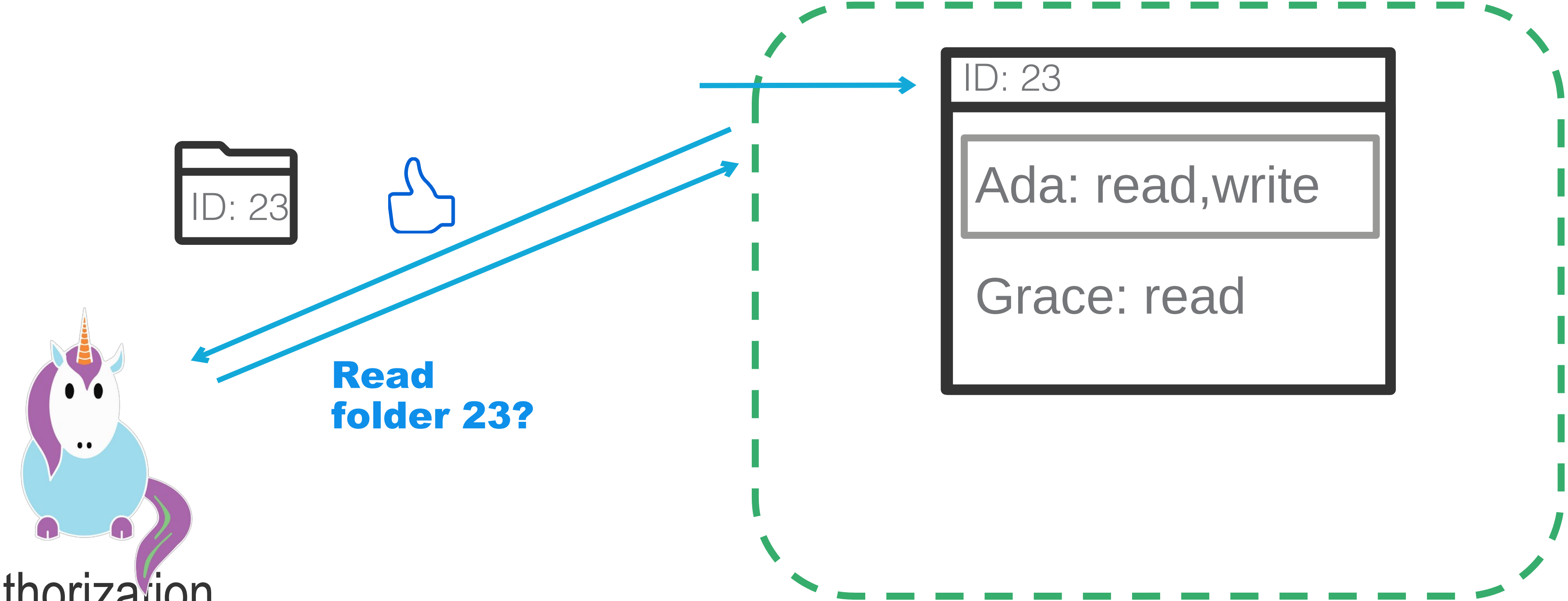
Ada: read,write

Grace: read

Ada: read

Grace: read

ACLs: Fast Lookup



ID: 23

Read folder 23?

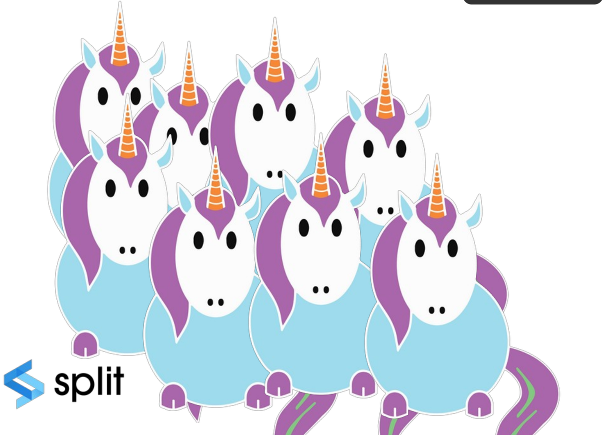
ID: 23

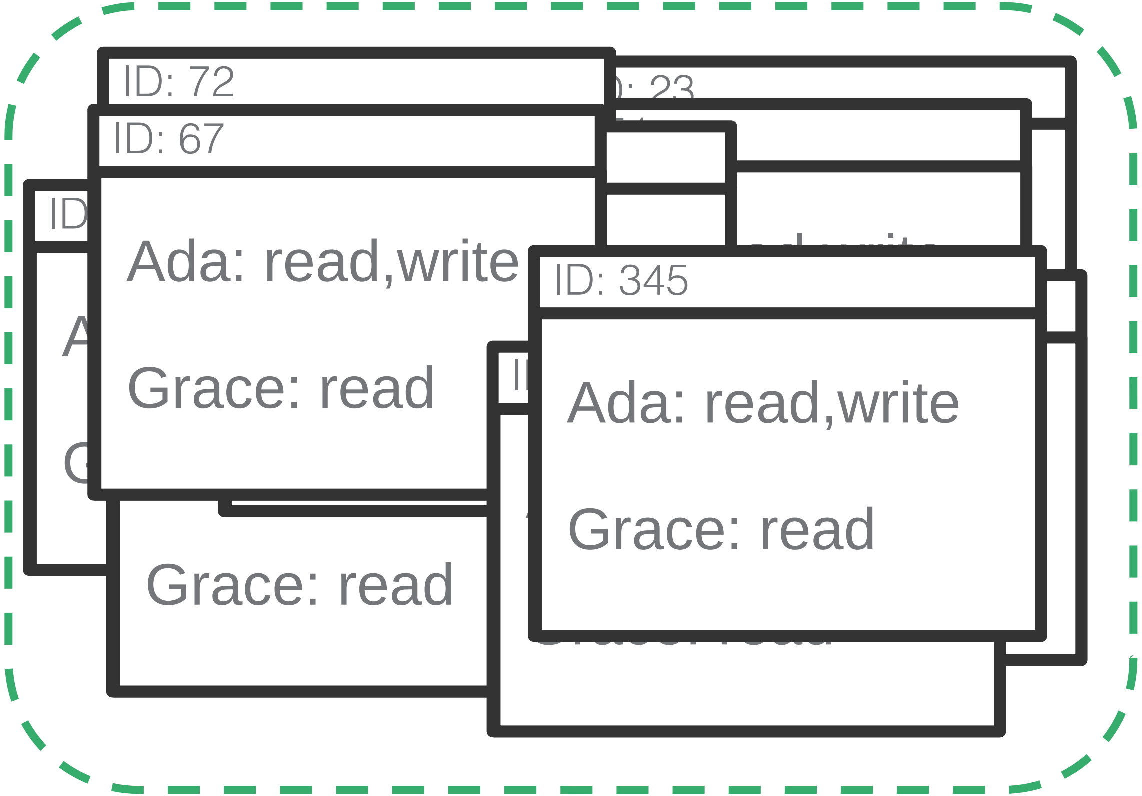
Ada: read,write

Grace: read

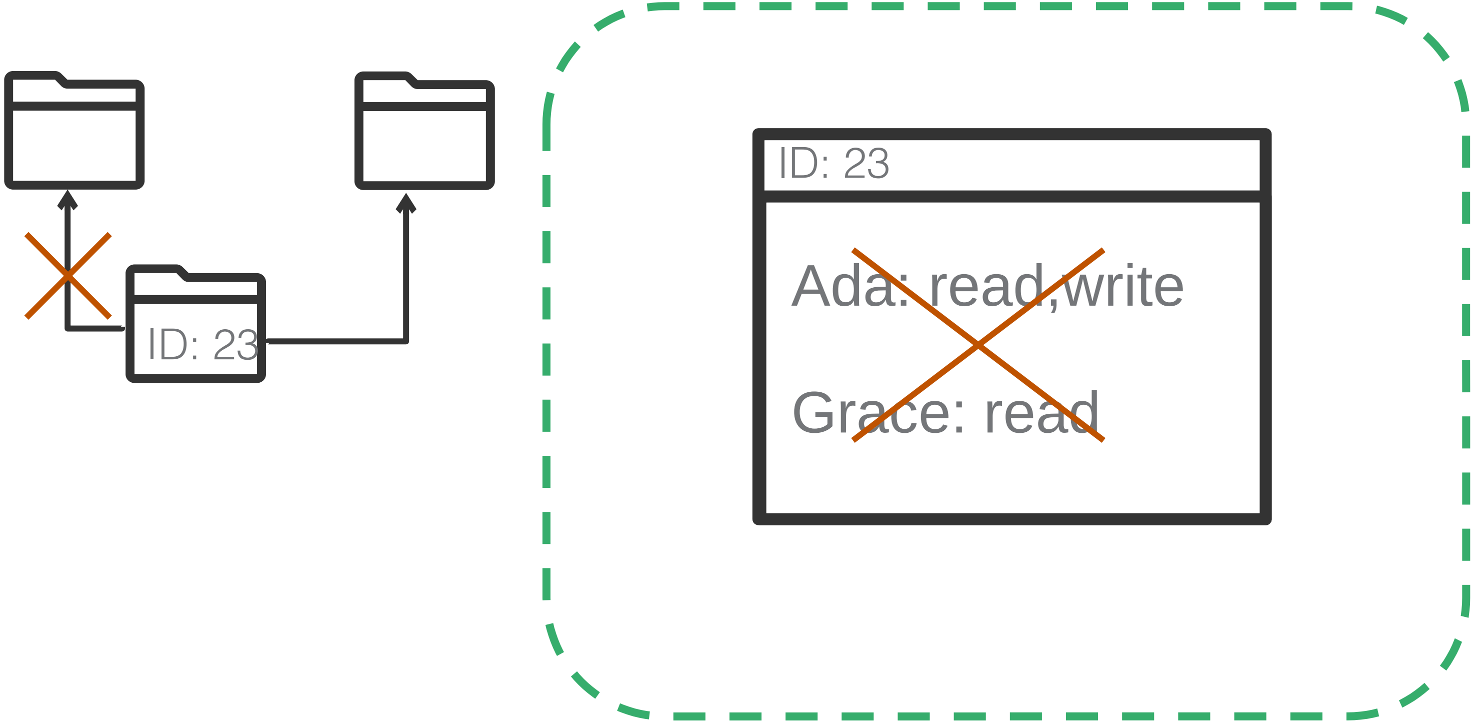
ACLs: Storage Explosion

ID: 23
ID: 91
ID: 72
ID: 51
ID: 65





ACLs: Slow Update

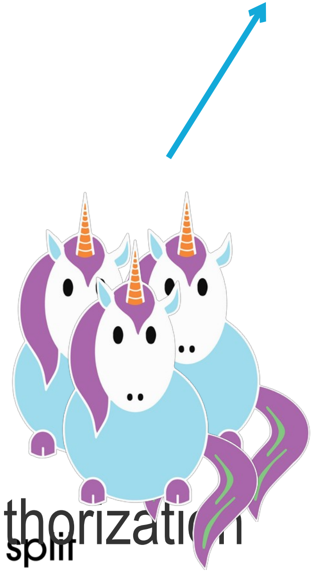


ID: 23

ID: 23

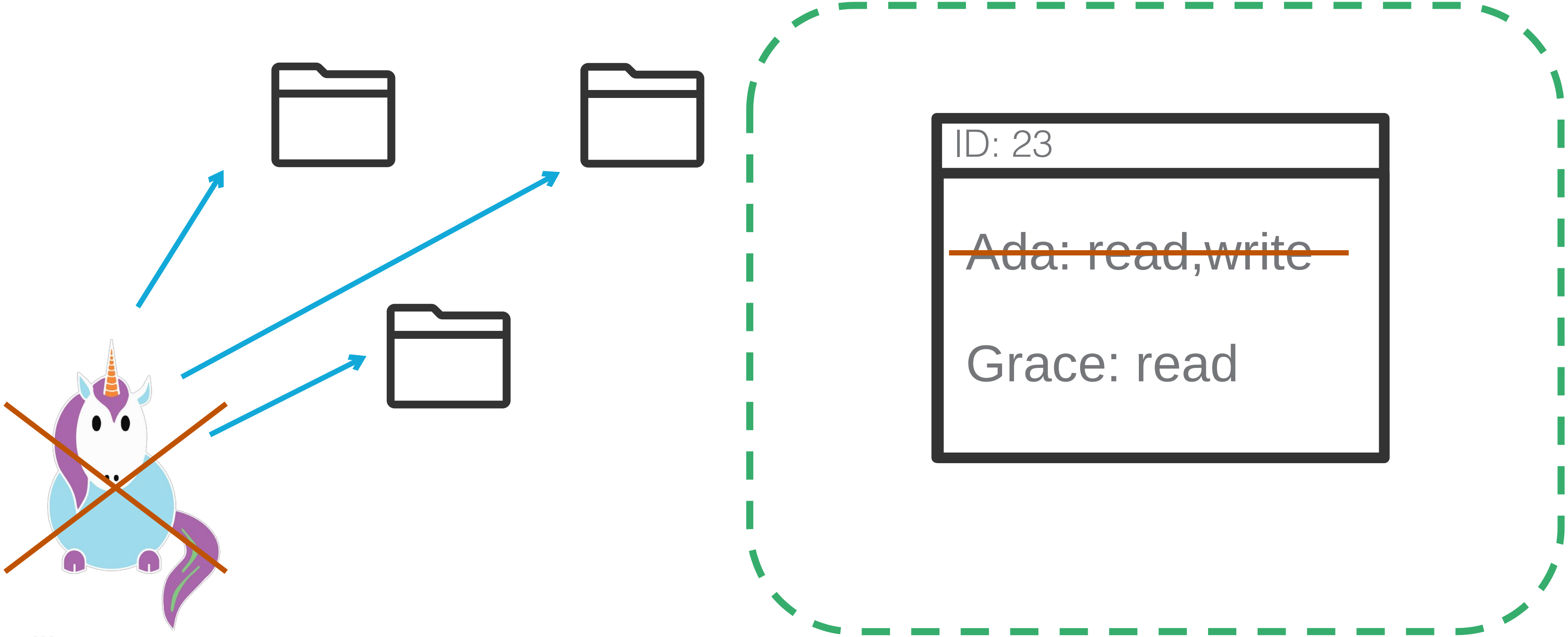
~~Ada: read,write~~

~~Grace: read~~



Authorization

ACLs: Slow Update



ID: 23

~~Ada: read,write~~

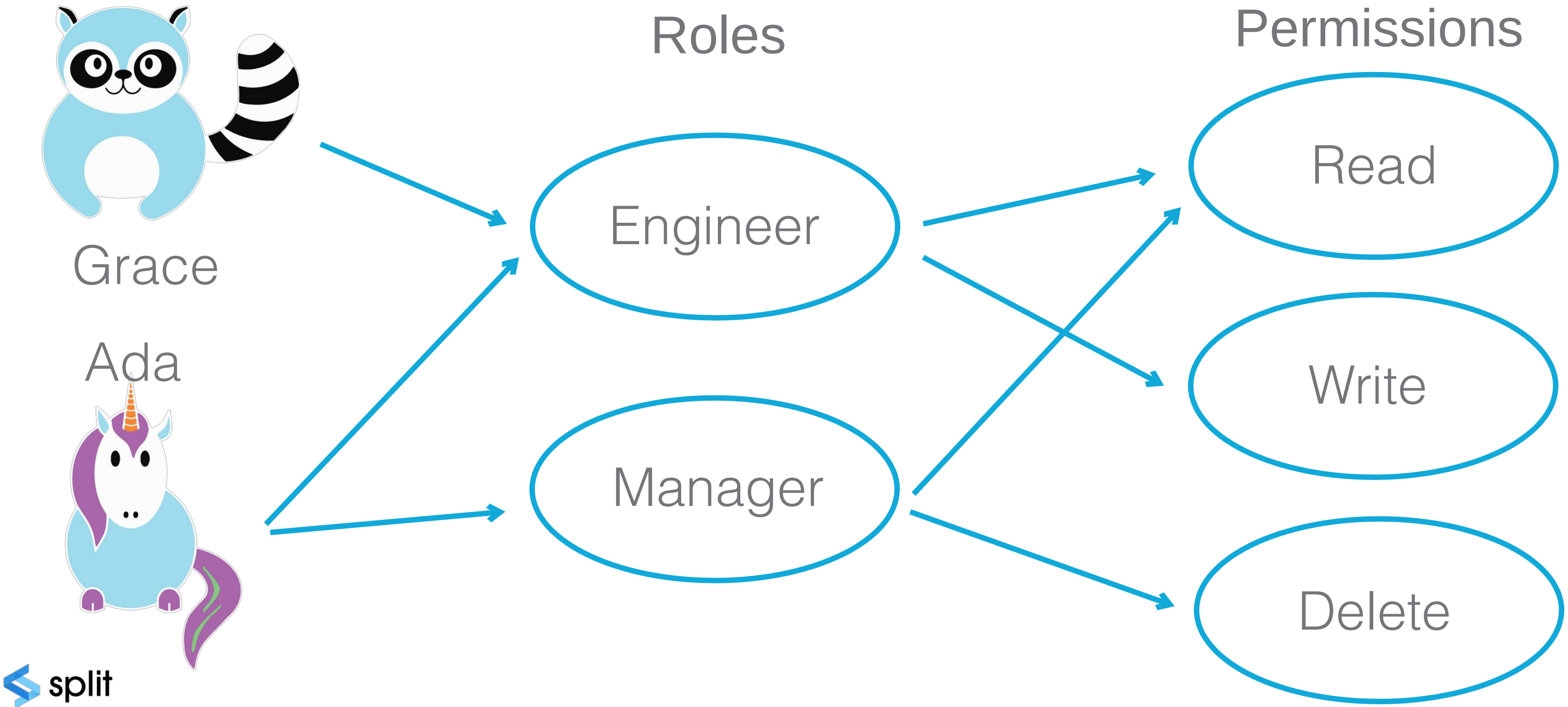
Grace: read

Types of Access Control

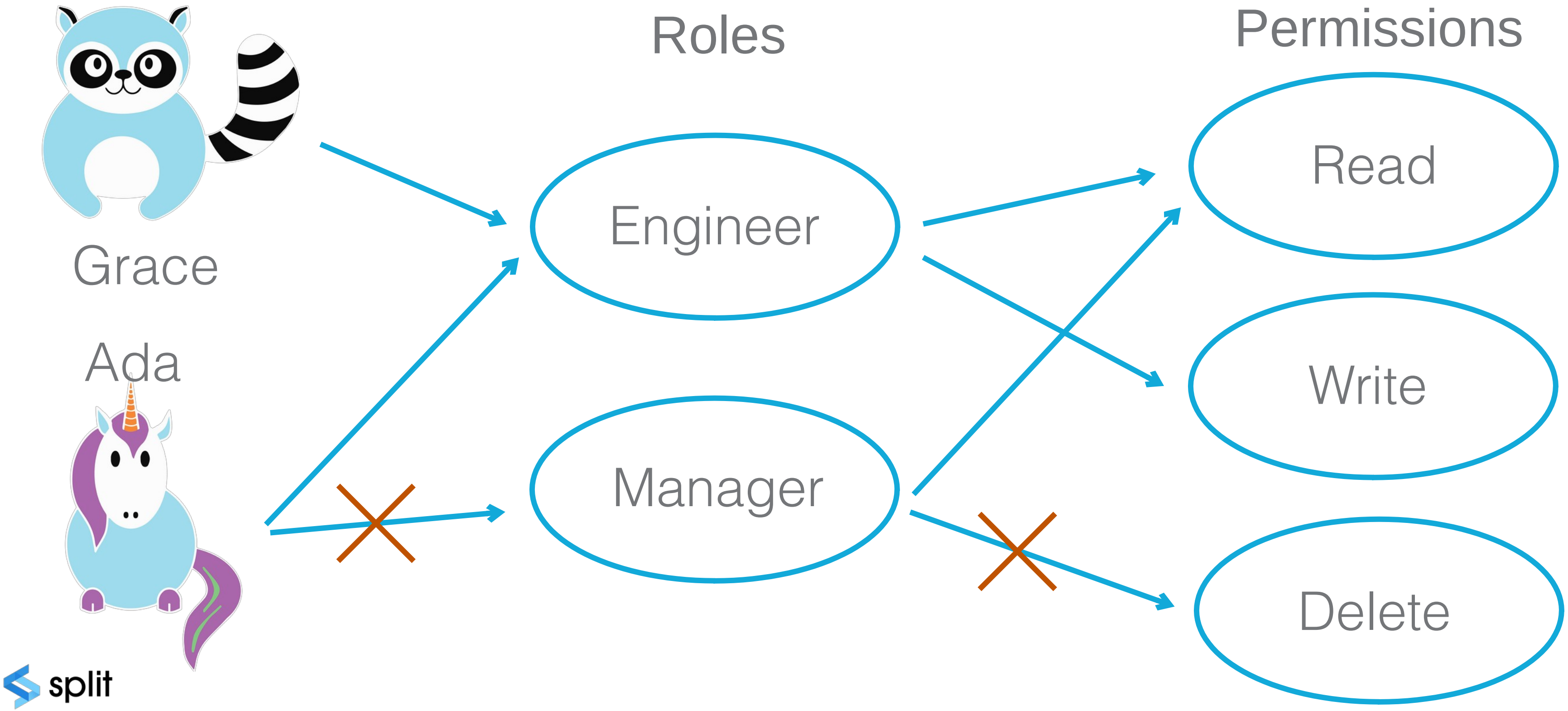
RBAC

DEVOPS WORLD
by CloudBees

RBAC (Role Based Access Control)



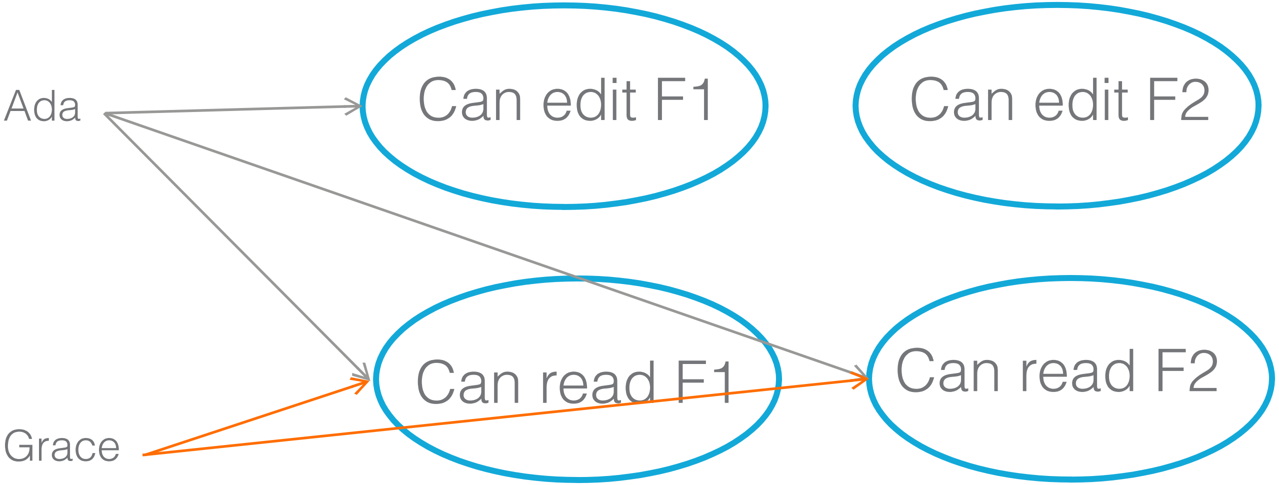
RBAC: Fast Update



split

RBAC cons: Role Explosion

	F1	F2
Ada	Read, Write	Read
Grace	Read	Read

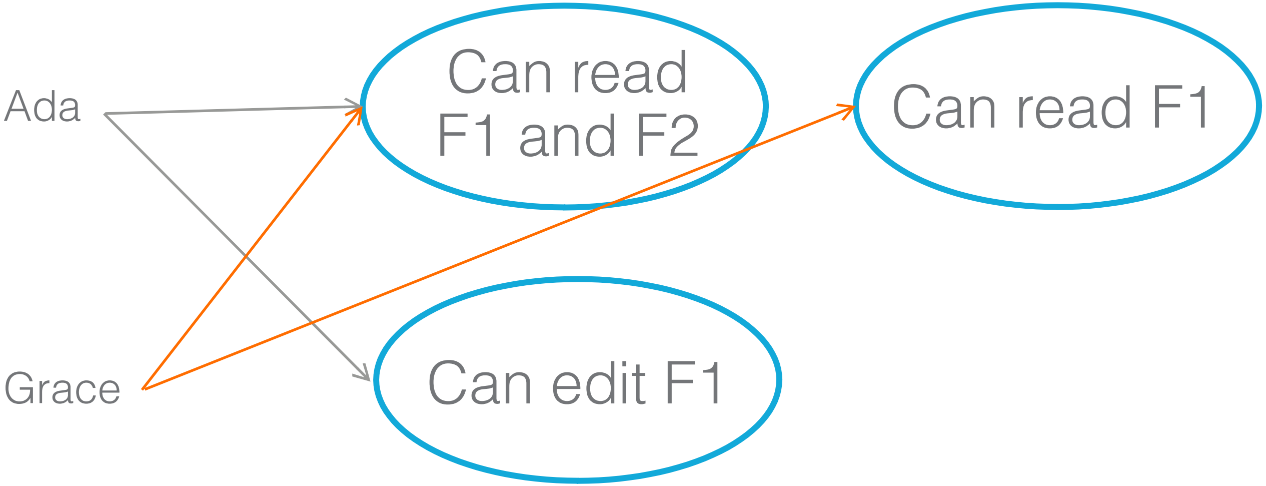


Roles

RBAC cons: Role Explosion

	F1	F2
Ada	Read, Write	Read
Grace	Read	~~Read~~

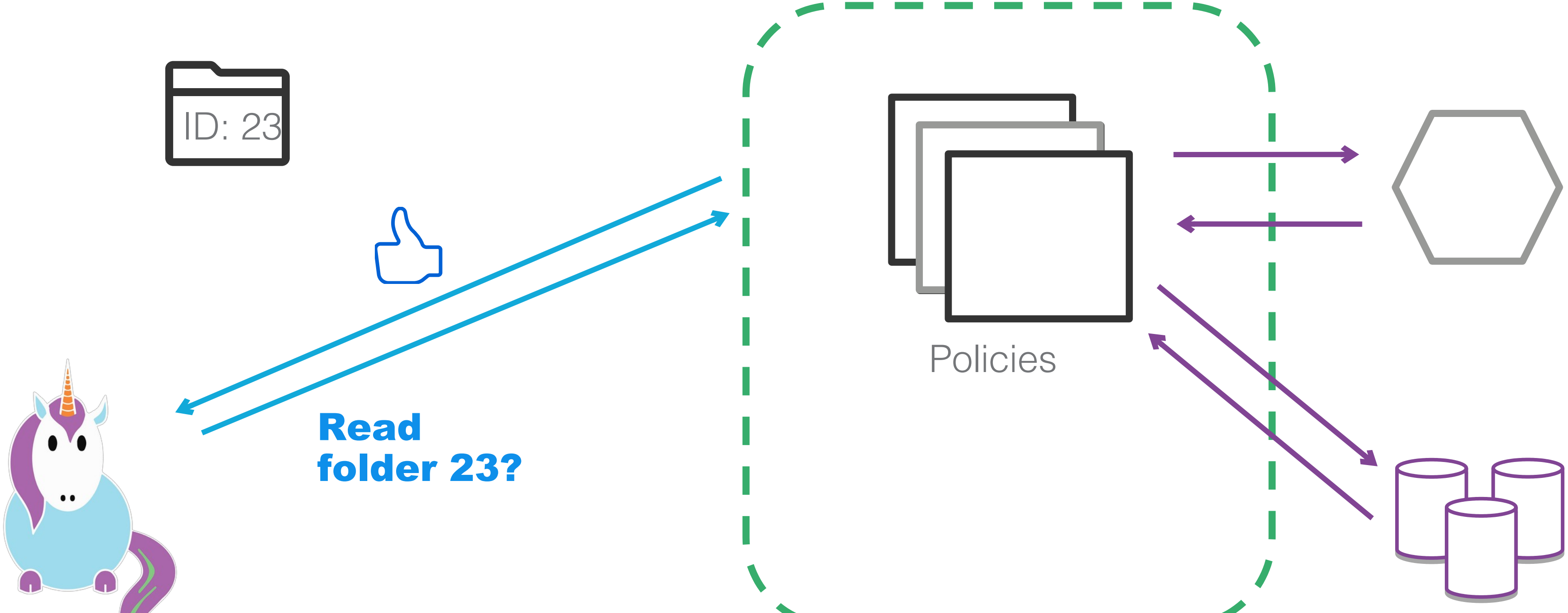
Roles



Types of Access Control

ABAC

ABAC (Attribute Based Access Control)



Authorization

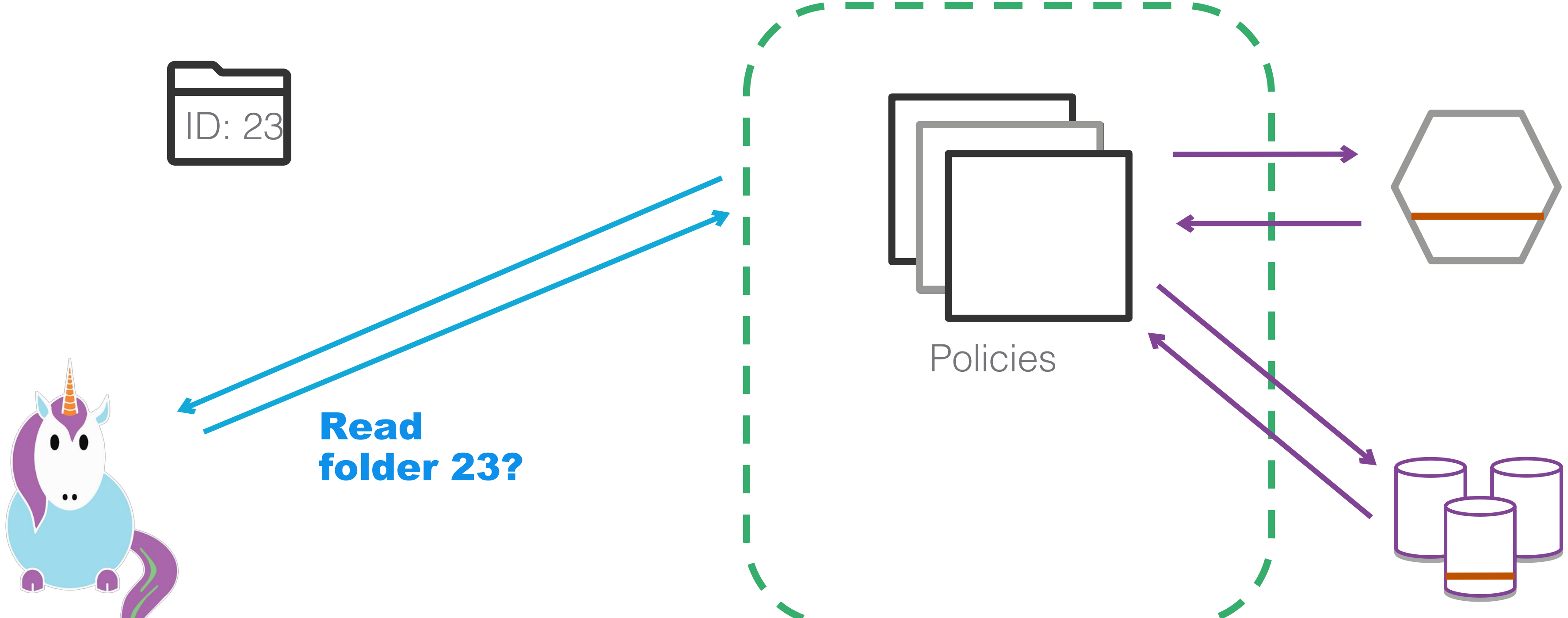
split

ABAC: Requests & Policies

```
User with ID 123
   wants to VIEW file with ID 456
```

```
If the action is VIEW
   And the enterprise of the resource
   is the same as the enterprise of the subject
Then PERMIT access
Else DENY
```

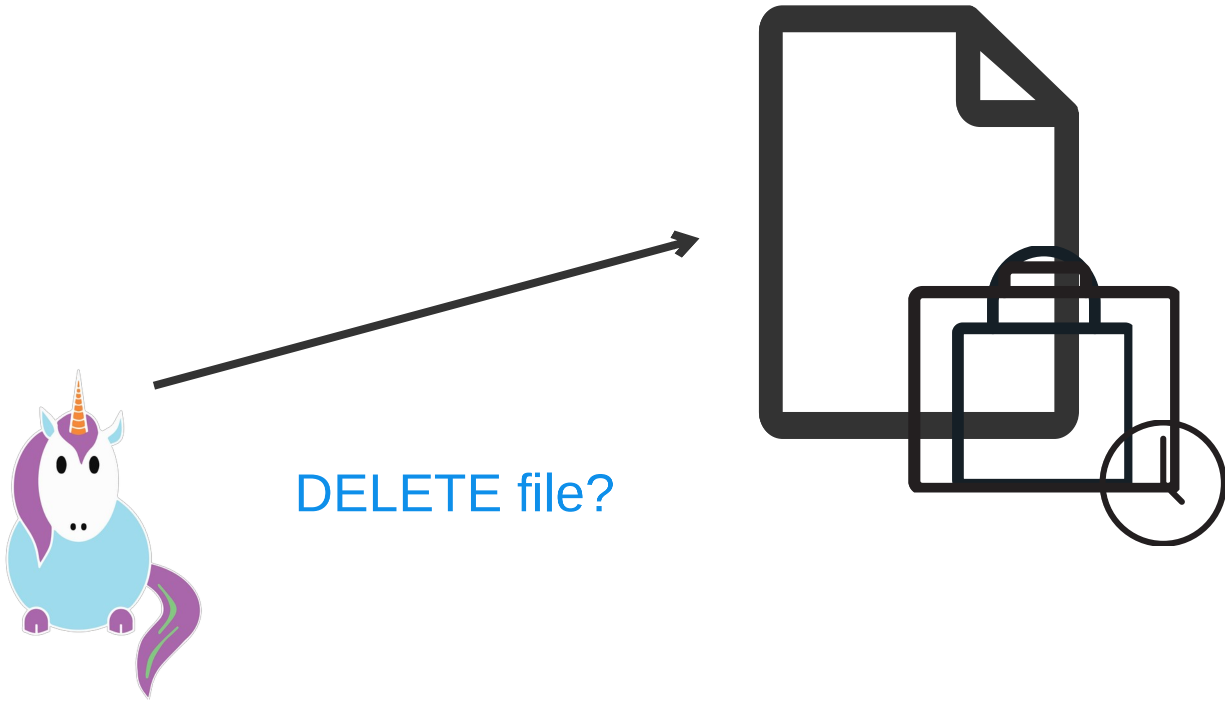
ABAC: Immediate Update



Read folder 23?

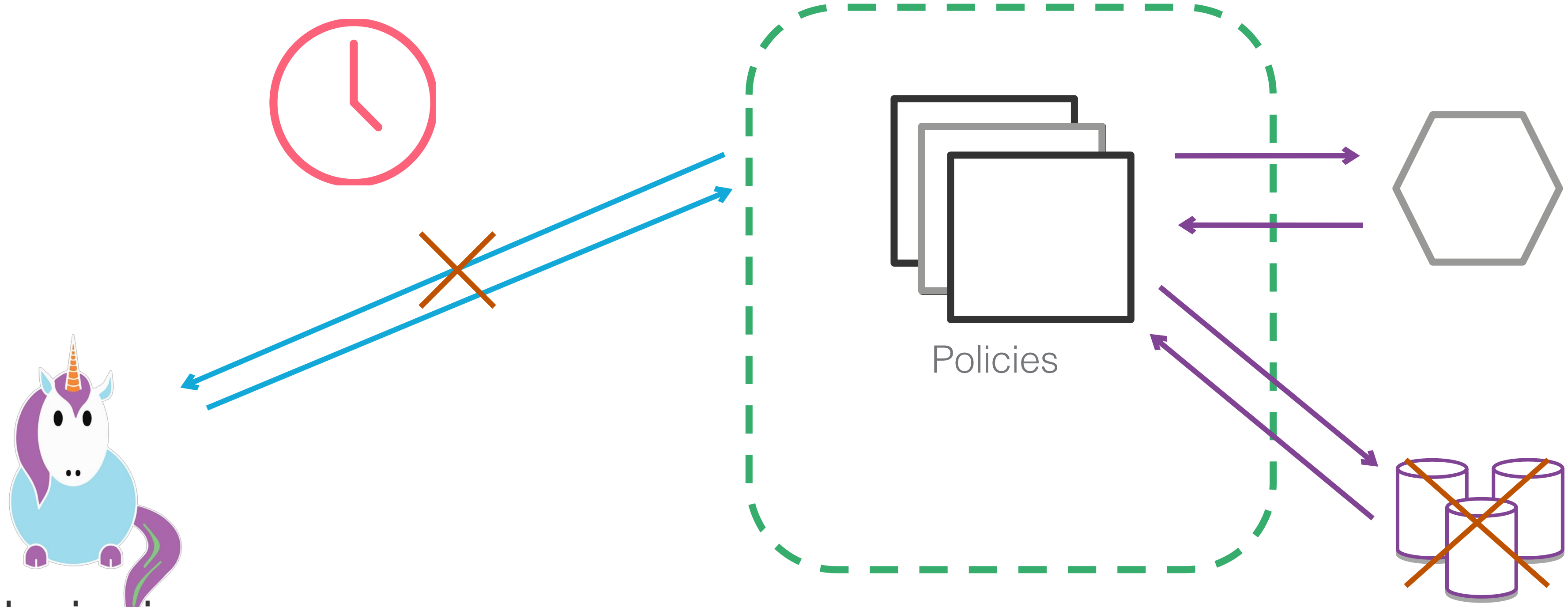
Authorization

ABAC: Handles Complex Use-cases



DELETE file?

ABAC: Slow Lookup, Dependencies



Authorization

Our Choice: ABAC

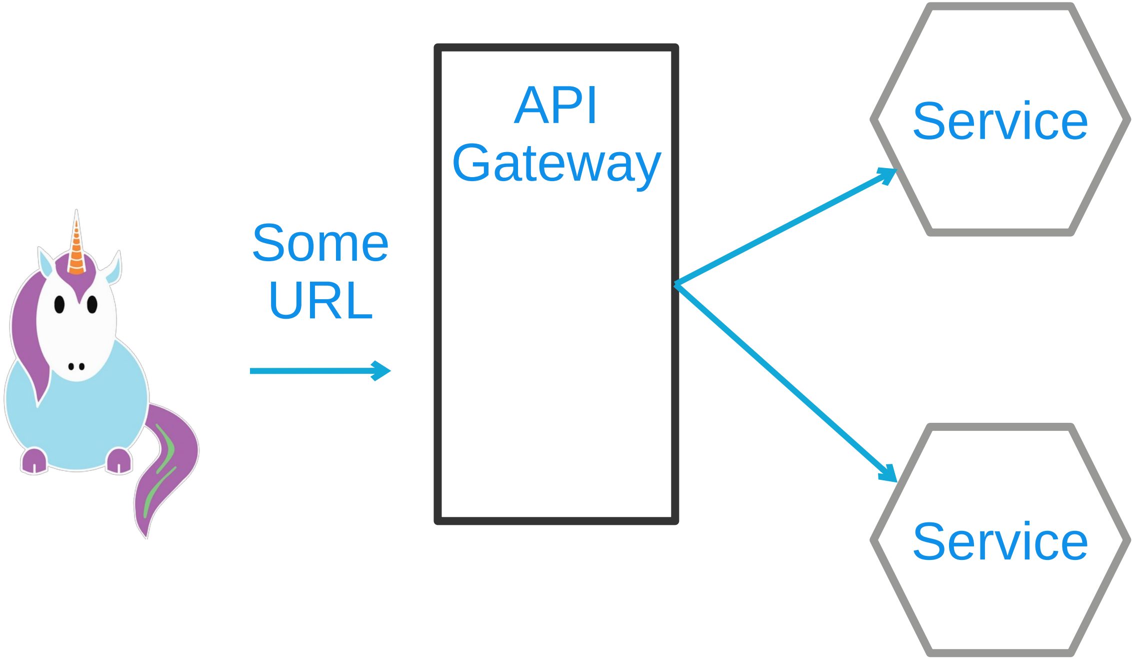
Why ABAC?

- Industry standard
- No permission update lag
- Space efficient
- Best fits our use-cases - ACLs/RBAC too simple
    - Because we want to allow access to objects per user, we would have too many lists/roles
- Can still expose simpler permissions features to customers

Typical Architecture

DEVOPS WORLD by CloudBees

Typical Architecture



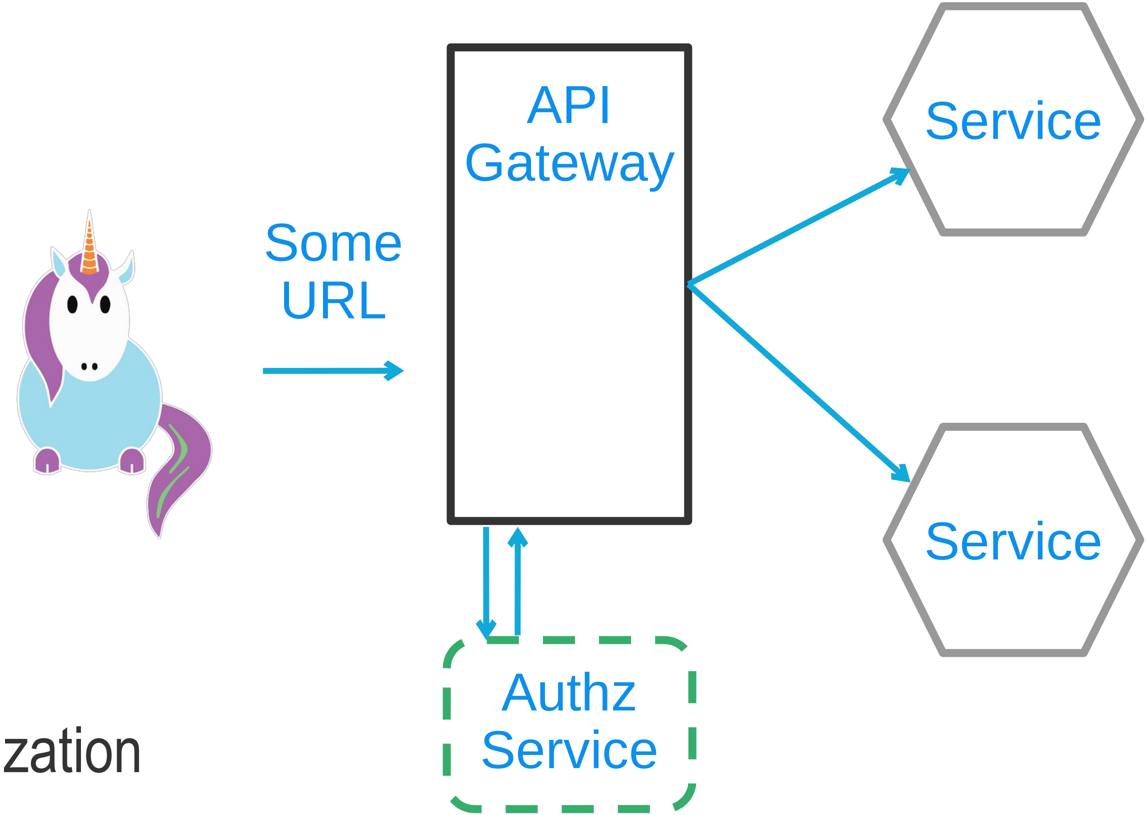
Some URL

API Gateway

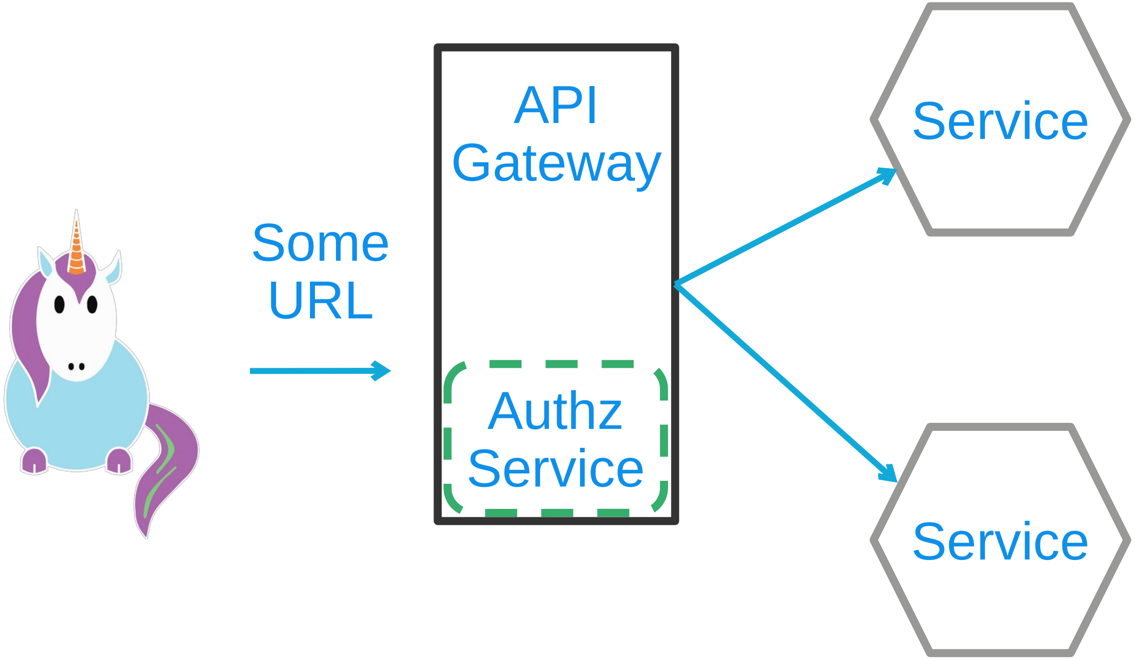
Service

Service

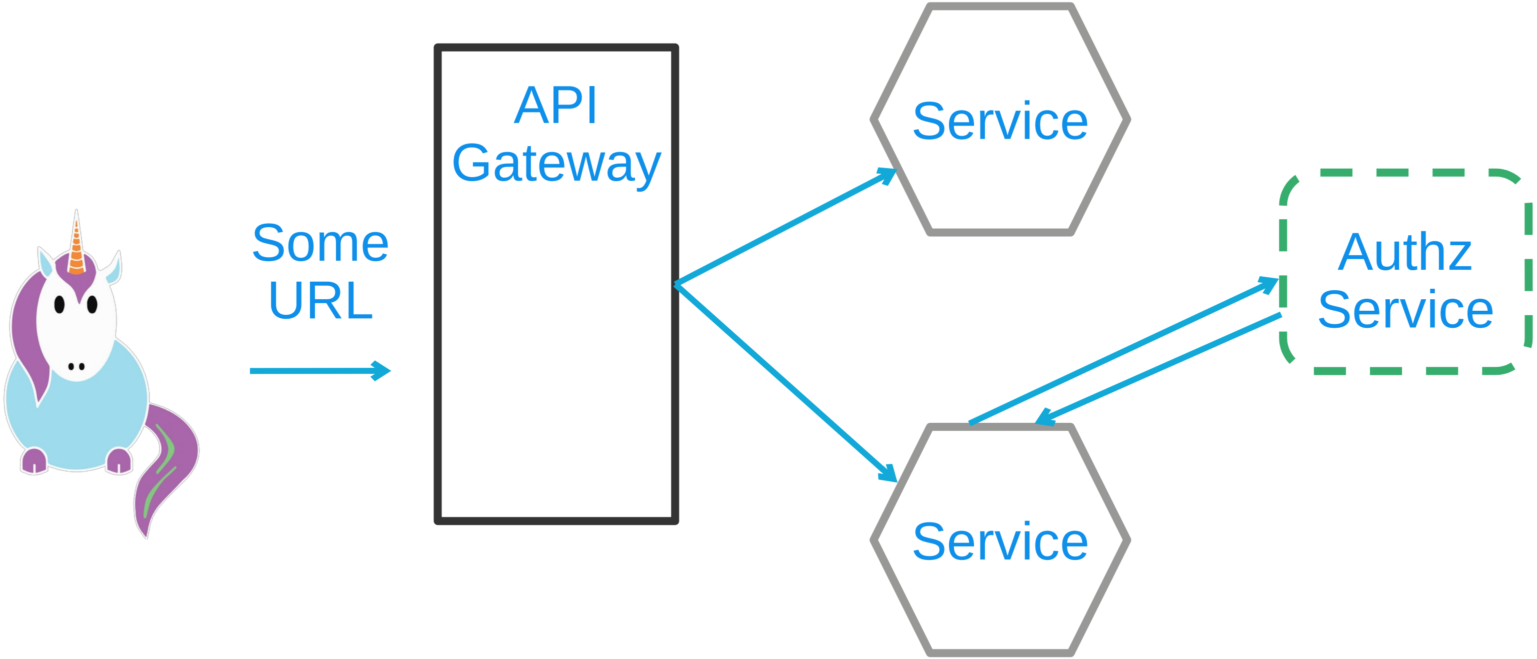
Typical Architecture: API Gateway



Typical Architecture: API Gateway

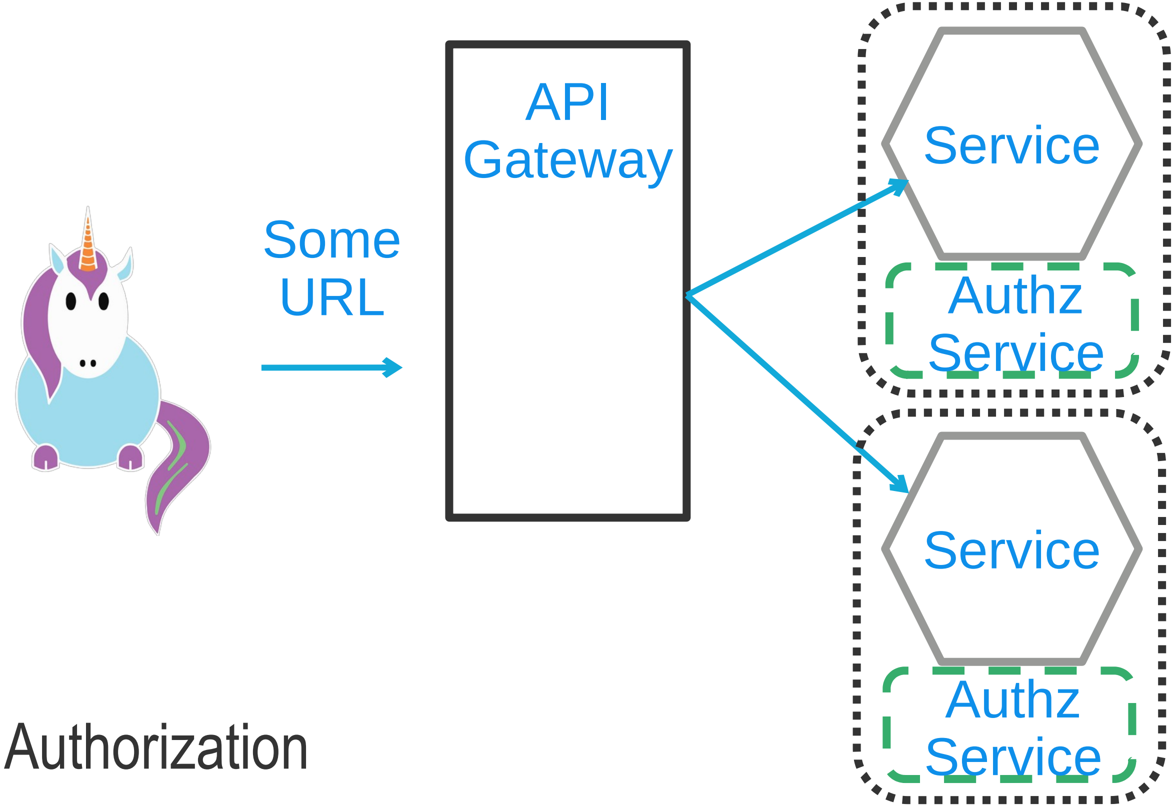


Typical Architecture: Separate Service



split Authorization

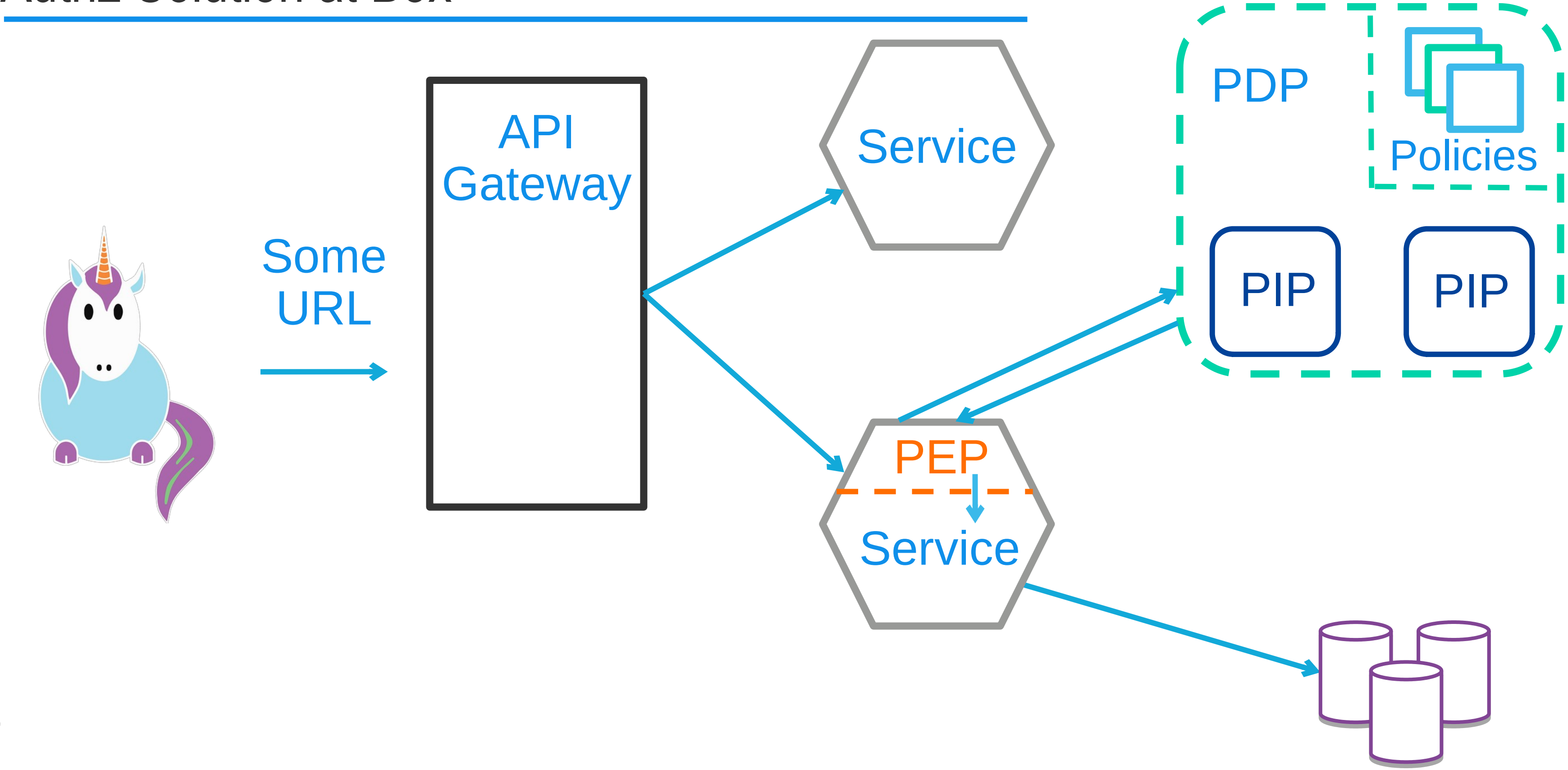
Typical Architecture: Side Car



split Authorization

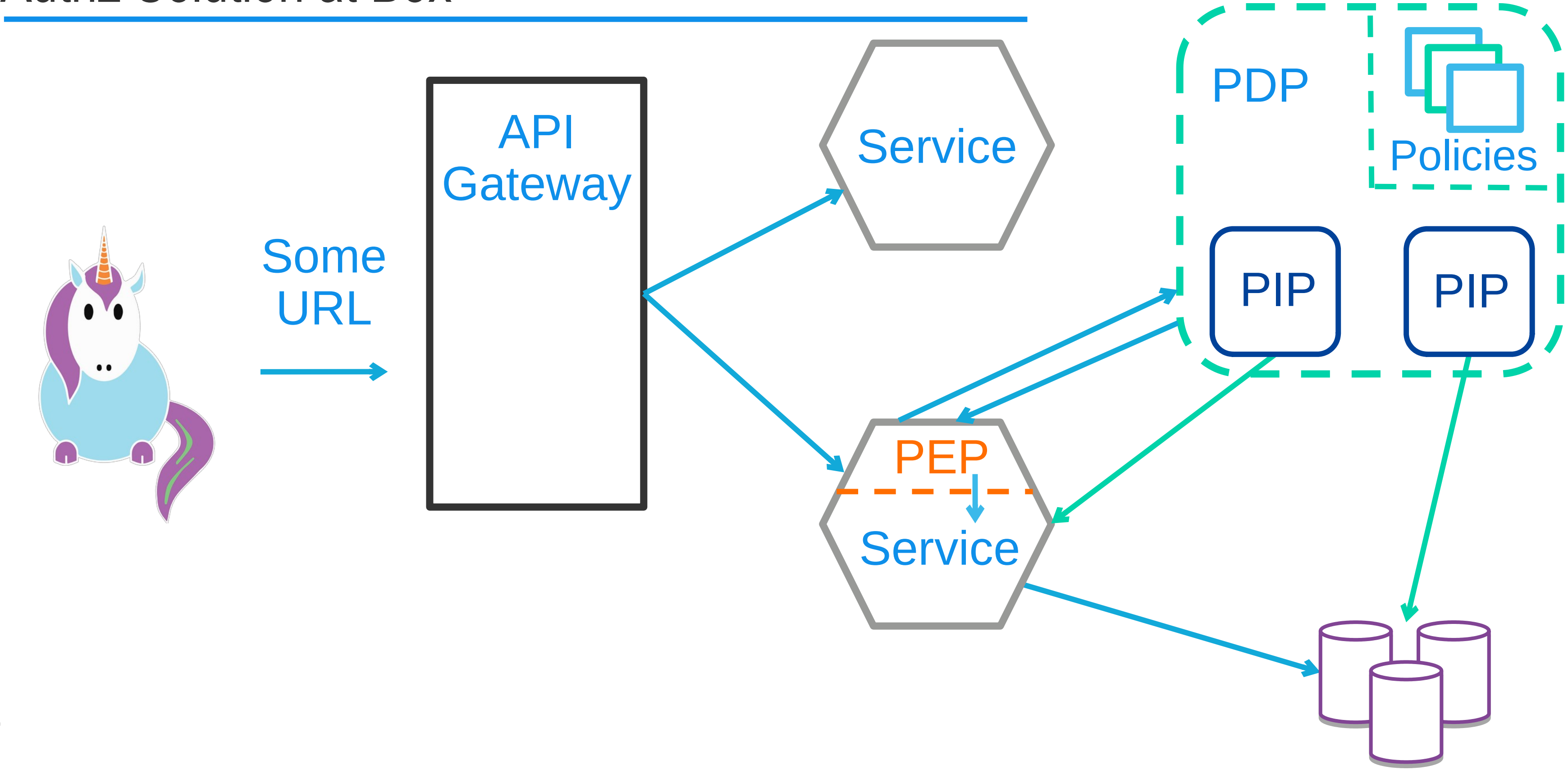
Implementation at Box

Authz Solution at Box



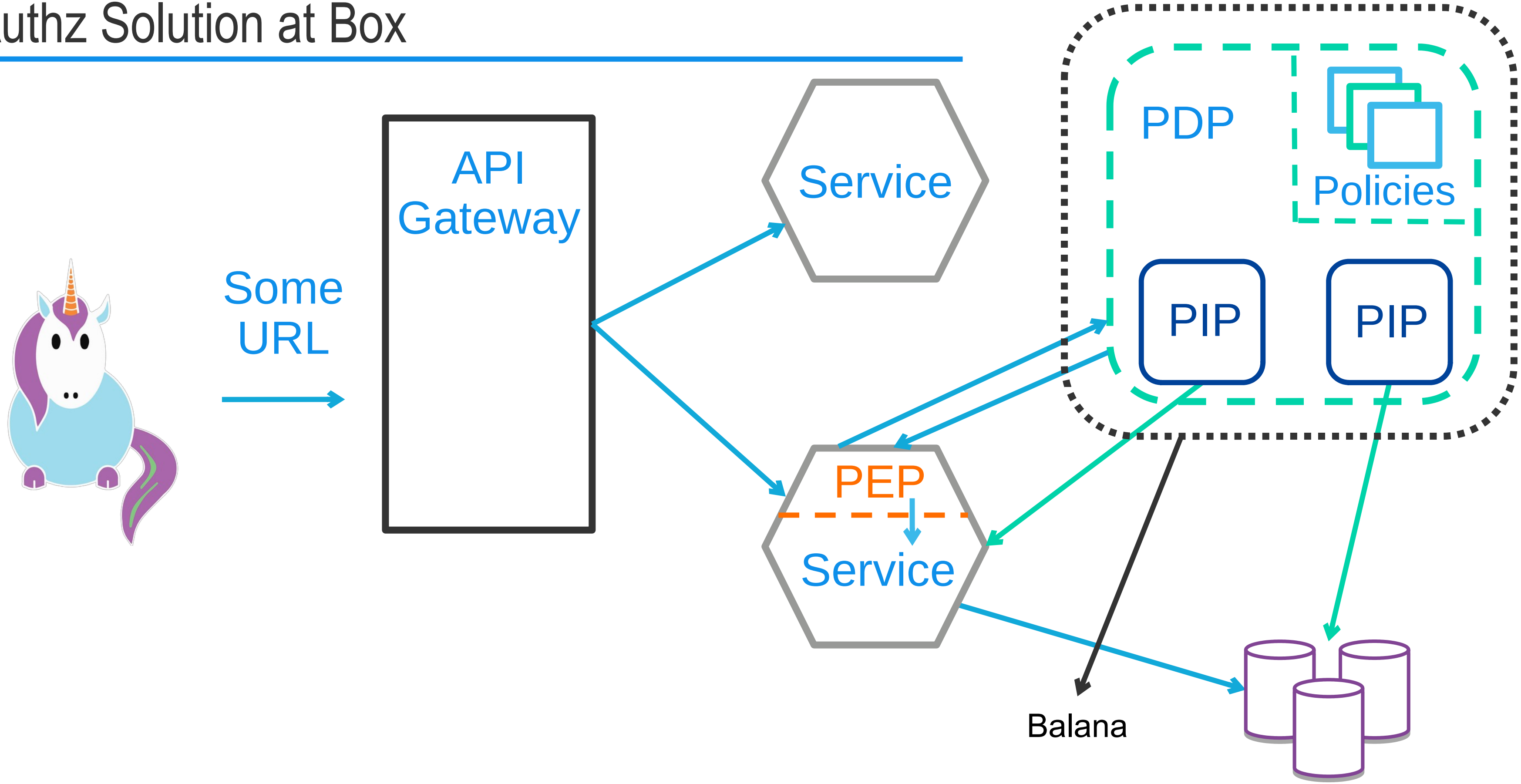
split

Authz Solution at Box



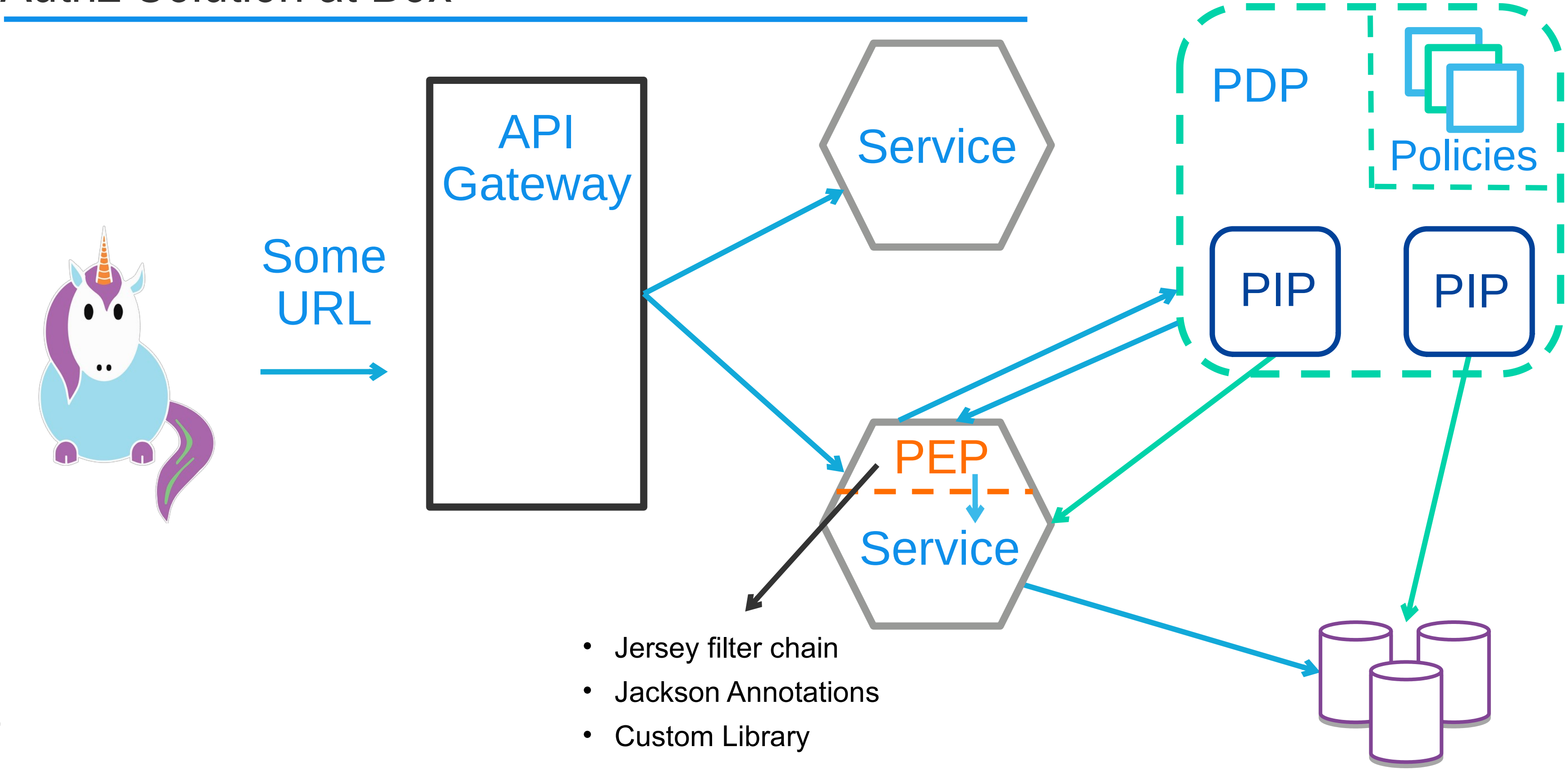
split

Authz Solution at Box



split

Authz Solution at Box



- Jersey filter chain
- Jackson Annotations
- Custom Library

Thank You!

Joy Ebertz

@jkebertz

DEVOPS WORLD by CloudBees