

Serverless Data Processing (CSCI 5410)

Dr. Saurabh Dey

Images and contents used in these slides are from web search and/or text books, and are used for academic purposes only

This content is protected and may not be shared, uploaded, or distributed

Outline


AWS Identity and Access
Management

Amazon Resource Name



Identifying an IAM user

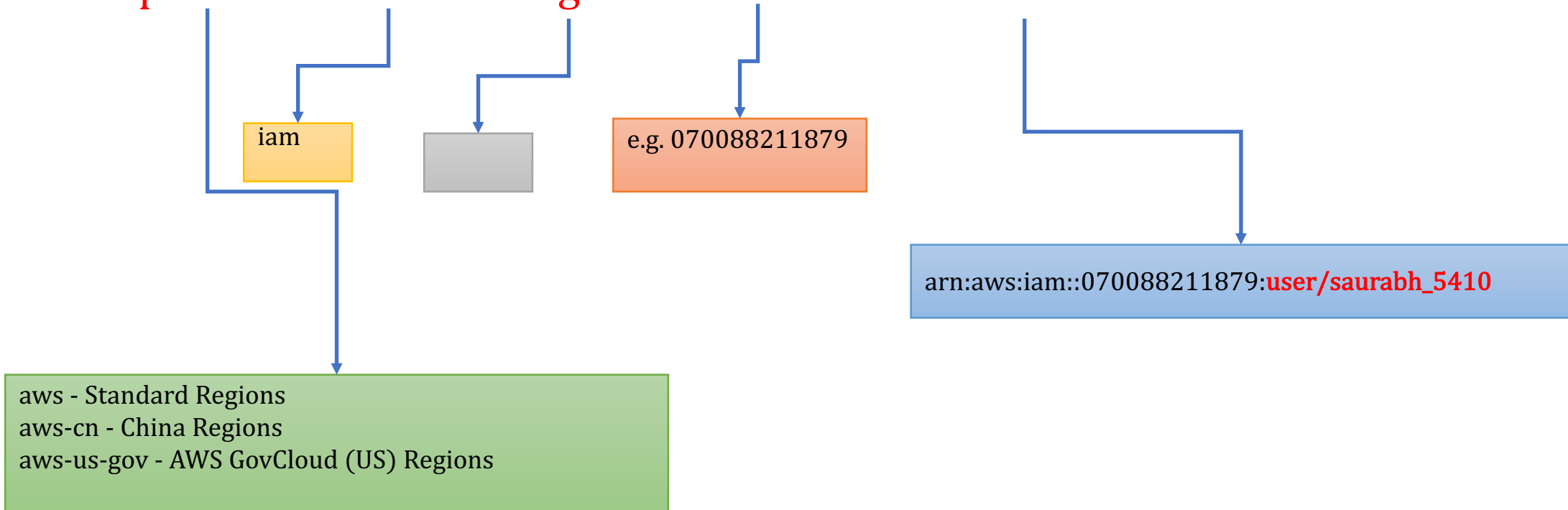
- A friendly name of the user is added at the time of user creation
- An Amazon Resource Name (ARN) for the user
- A unique identifier for the user

User ARN	arn:aws:iam::070088211879:user/saurabh_5410 
Path	/
...	...

ARN: Amazon Resource Name

- ARN has a specific format. It is required by the permission policy language

arn: **partition** : **service** : **region** : **account** : **resource**



Syntax of ARNs

arn:aws:iam::*account-id*:root

arn:aws:iam::*account-id*:user/*user-name-with-path*

arn:aws:iam::*account-id*:group/*group-name-with-path*

arn:aws:iam::*account-id*:role/*role-name-with-path*

arn:aws:iam::*account-id*:policy/*policy-name-with-path*

arn:aws:iam::*account-id*:instance-profile/*instance-profile-name-with-path*

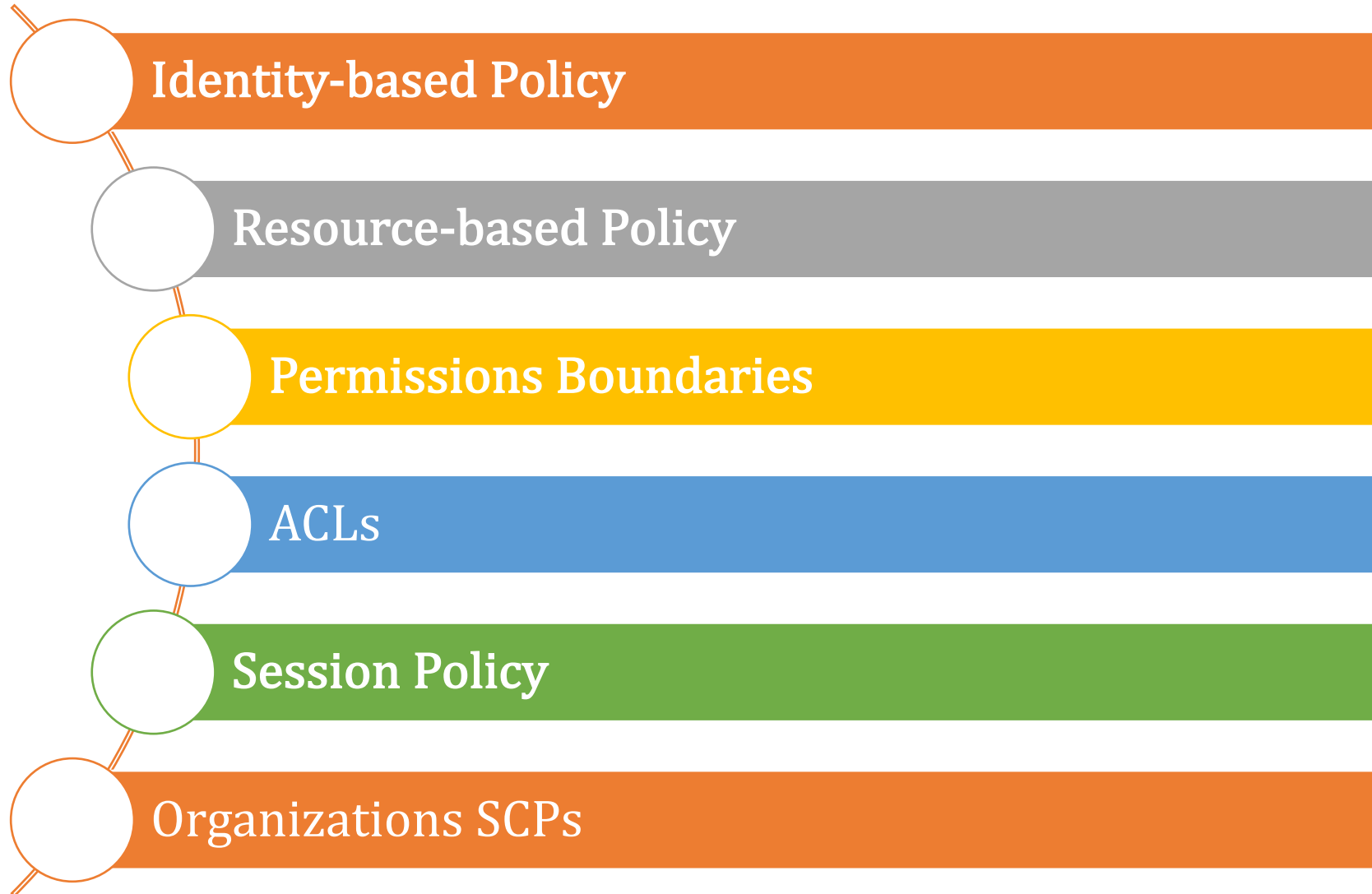
arn:aws:sts::*account-id*:federated-user/*user-name*

arn:aws:sts::*account-id*:assumed-role/*role-name*/*role-session-name*



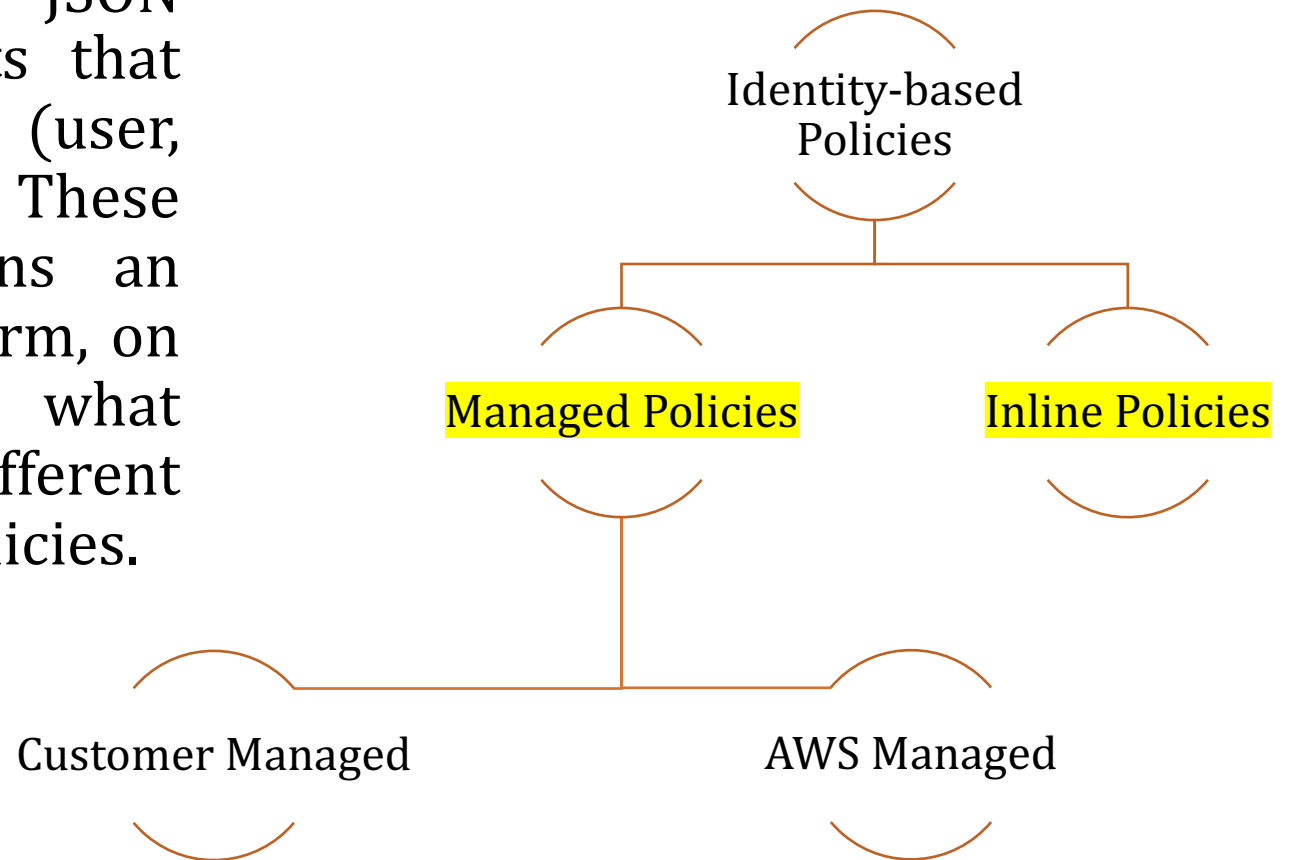
arn:aws:sts::357827796551:assumed-role/vocstartsoft/user497090=saurabh.dey@dal.ca

Policies and Permissions

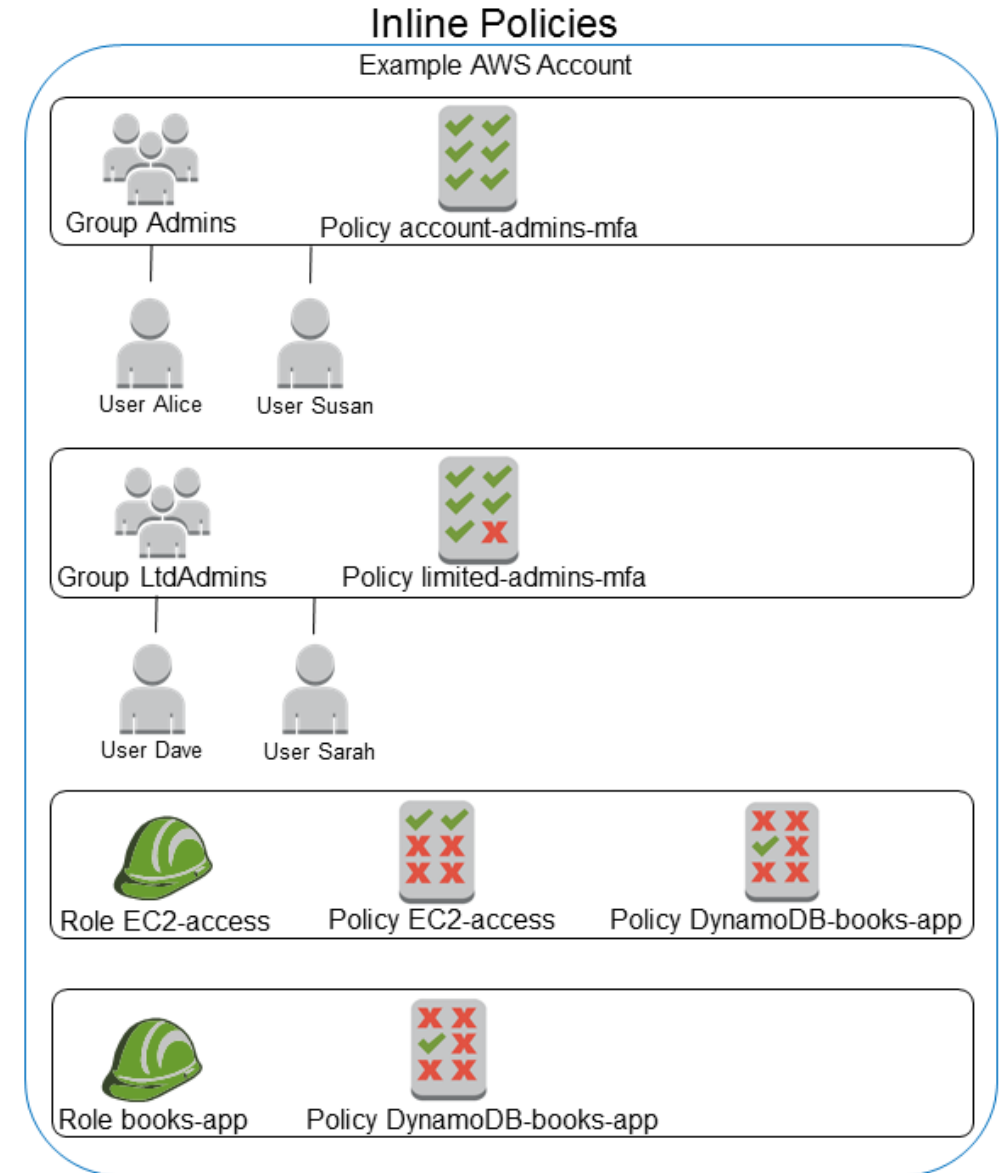
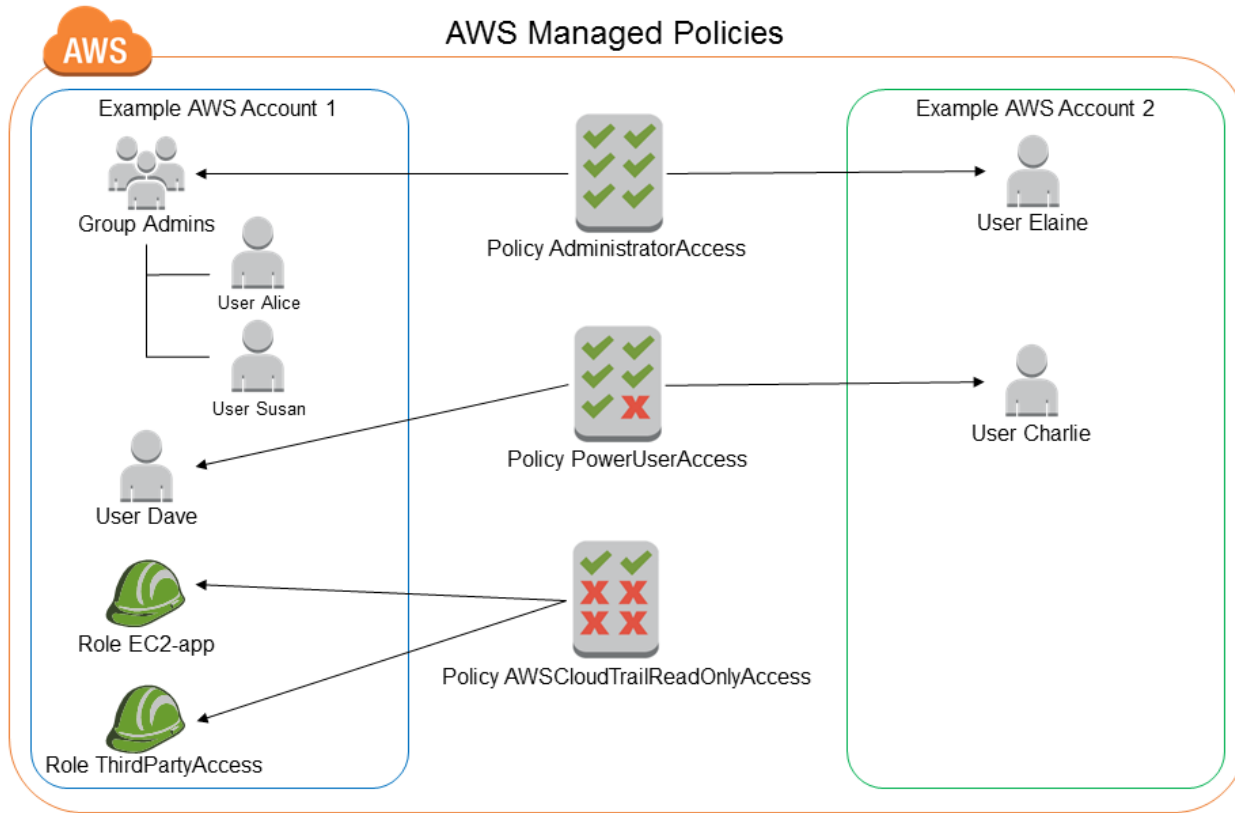


Identity-based Policies

- **Identity-based policies** are JSON permissions policy documents that you can attach to an identity (user, group of users, or role). These policies control what actions an entity (user or role) can perform, on which resources, and under what conditions. There are different categories of identity-based policies.



Managed vs Inline Policy



Resource-based Policies

- **Resource-based policies** are JSON policy documents that you attach to a resource such as an Amazon S3 bucket. These policies grant the specified principal permission to perform specific actions on that resource and defines under what conditions this applies. Resource-based policies are inline policies.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "S3:*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/bob"},
      "Resource": "*"
    }
  ]
}
```

ACLs (Access Control Lists)

- **Access control lists (ACLs)** are service policies that allow you to control which principals in another account can access a resource. ACLs cannot be used to control access for a principal within the same account. ACLs are similar to resource-based policies, although they are the only policy type that does not use the JSON policy document format.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  { 1
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      { 2
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

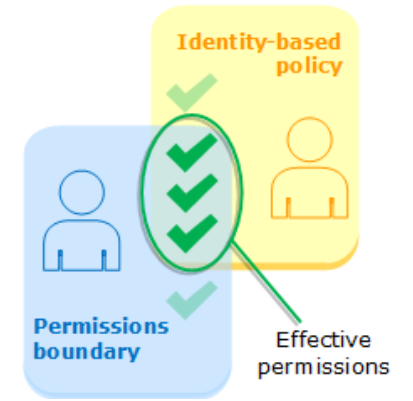
<https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html>

1 Owner Element
Identified by the canonical ID

2 Grant Element
(grantee, and permission)

Permission Boundary

- A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity. When you set a permissions boundary for an entity, the entity can perform only the actions that are allowed by both its identity-based policies and its permissions boundaries

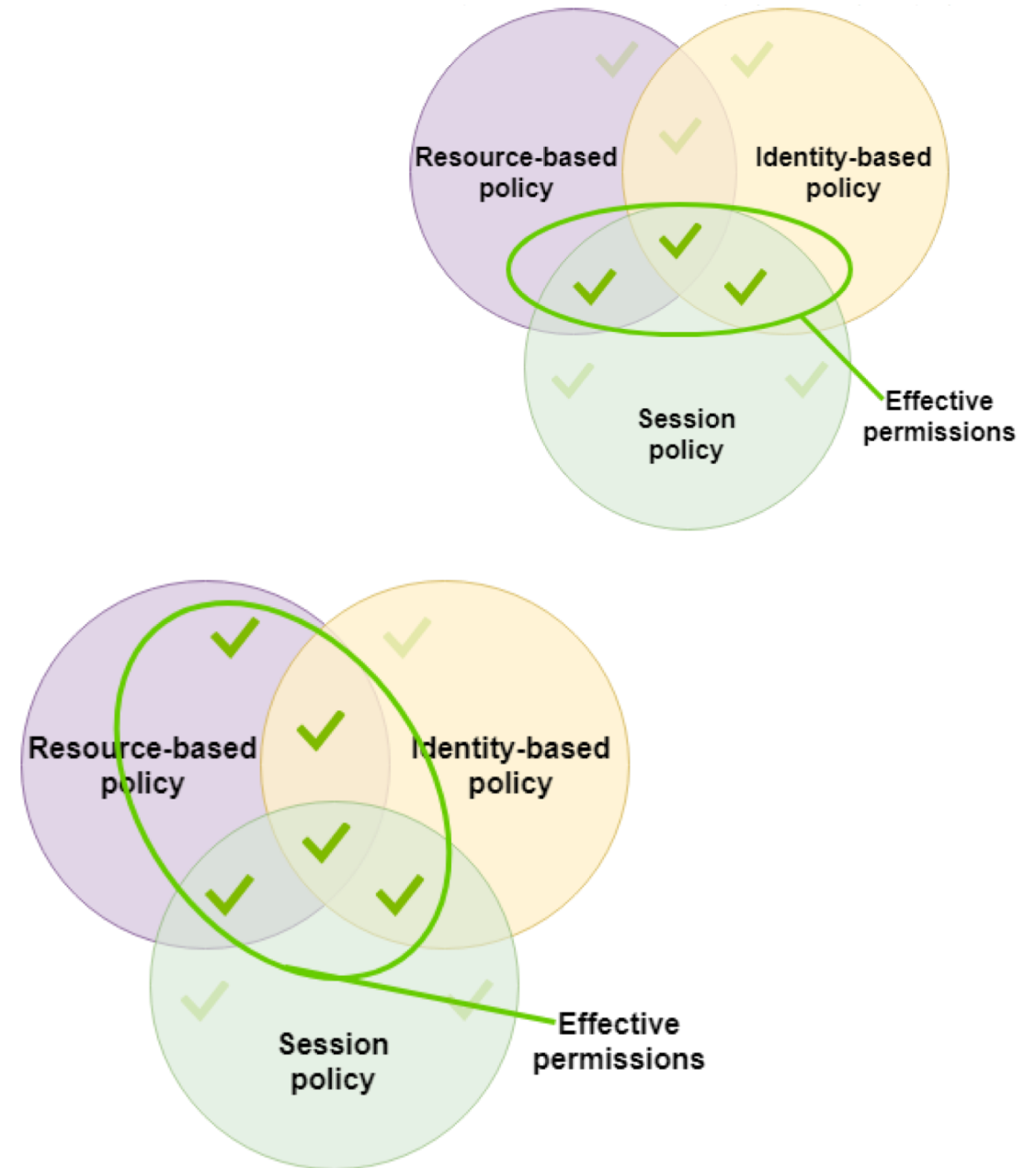


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "S3:*",
        "EC2:*"
      ],
      "Resource": "*"
    }
  ]
}
```

An entity Bob can manage only S3, and EC2

Session Policy

- **Session policies** are advanced policies that you pass in a parameter when you programmatically create a temporary session for a role or federated user. The permissions for a session are the intersection of the identity-based policies for the IAM entity (user or role) used to create the session and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow.



Questions to Consider

- To add access restriction to a file on S3 bucket, do we use resource-based policy, or identity-based policy?
- Can permission boundary limits the access and use of services that one can perform on AWS platform?

