IAM USER MANAGEMENT

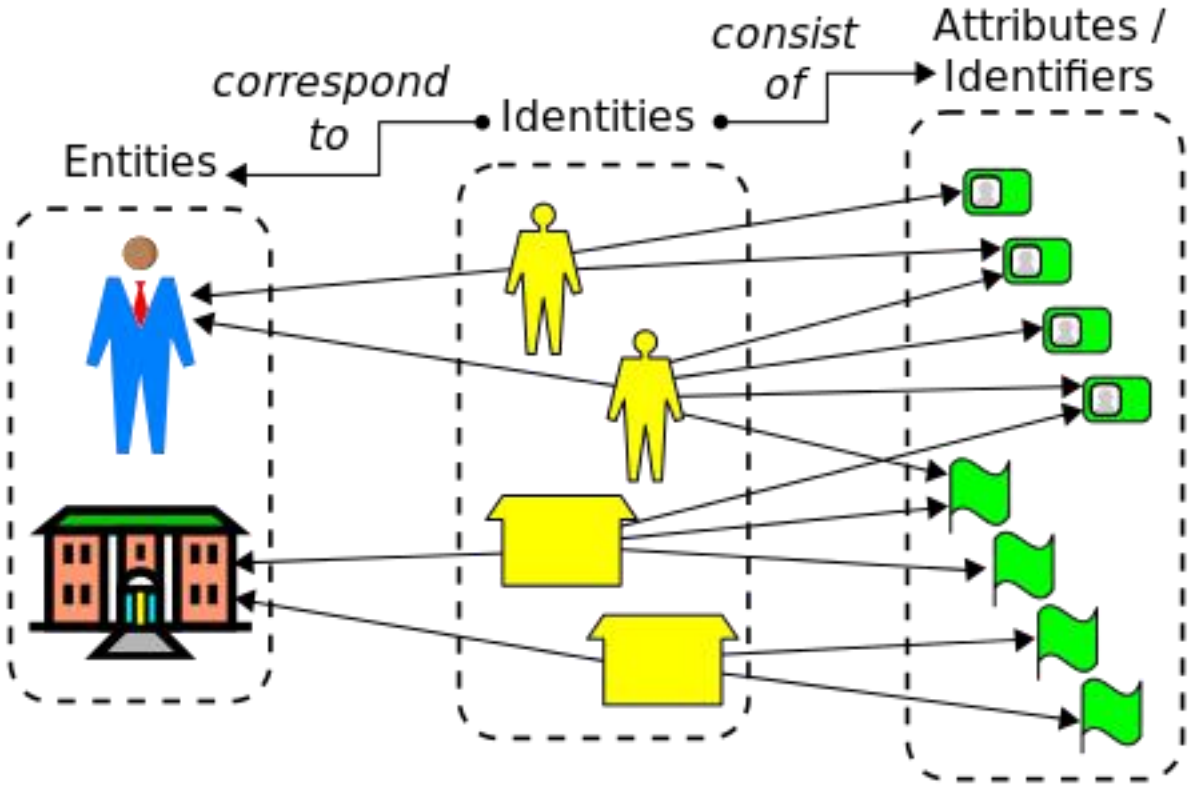
IAM ACCORDING TO AWS

IAM ACCORDING TO GCP

IAM ACCORDING TO AZURE

IAM - IDENTITY AND ACCESS MANAGEMENT

Common cloud ideas



IAM - IDENTITY AND ACCESS MANAGEMENT

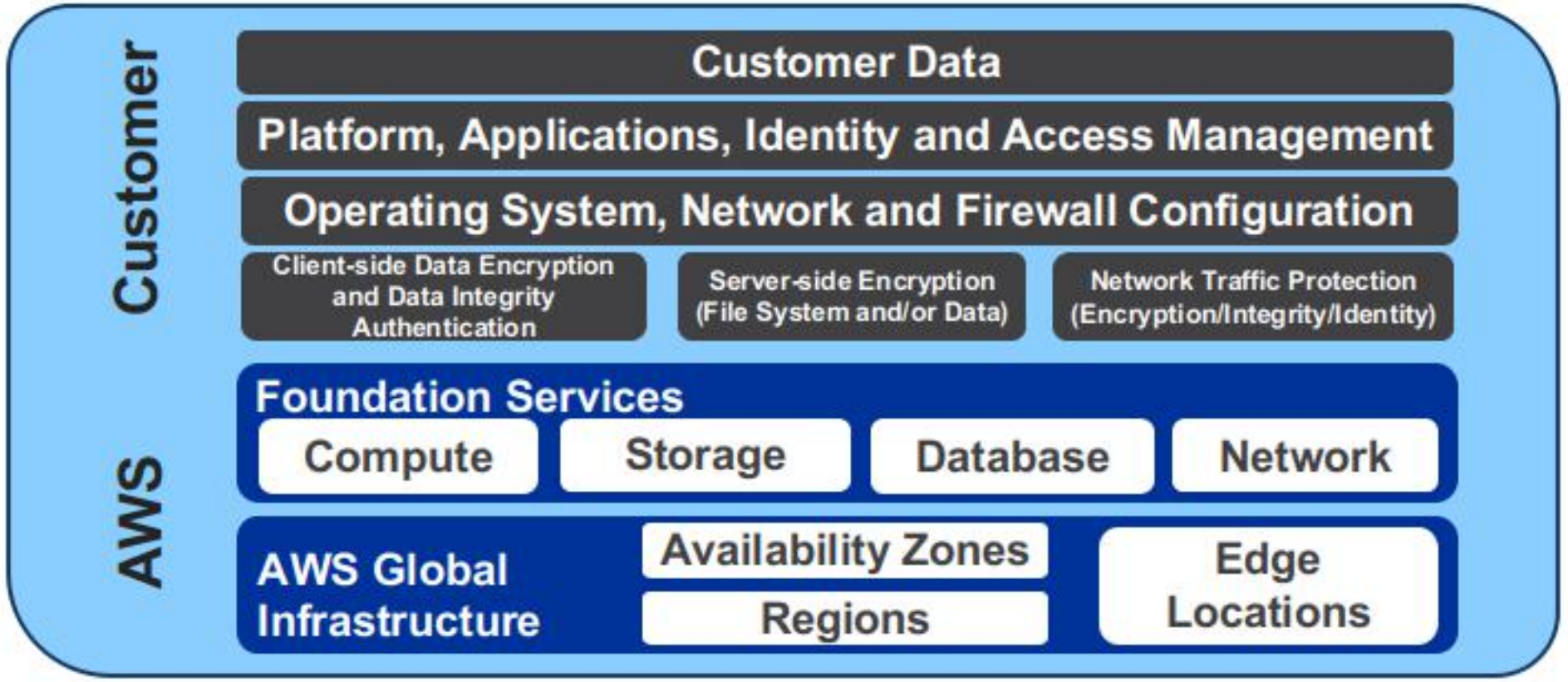
Identify, authenticate, and authorize individuals who will be utilizing IT resources

IAM, as a term, is used across clouds

In each cloud, IAM is implemented with a different structure

- Organizations
- Projects
- Permissions

SHARED SECURITY RESPONSIBILITY



data

PHYSICAL SECURITY

24/7 trained security staff

Data centers in nondescript and undisclosed facilities

Two-factor authentication for authorized staff

Authorization for data center access

Separate logical and physical access

PHYSICAL SECURITY VIDEO

https://www.youtube.com/watch?v=kd33UVZhnAA

CERTIFICATIONS AND ACCREDITATIONS

FERPA

- https://aws.amazon.com/blogs/security/ferpa-compliance-in-the-aws-cloud

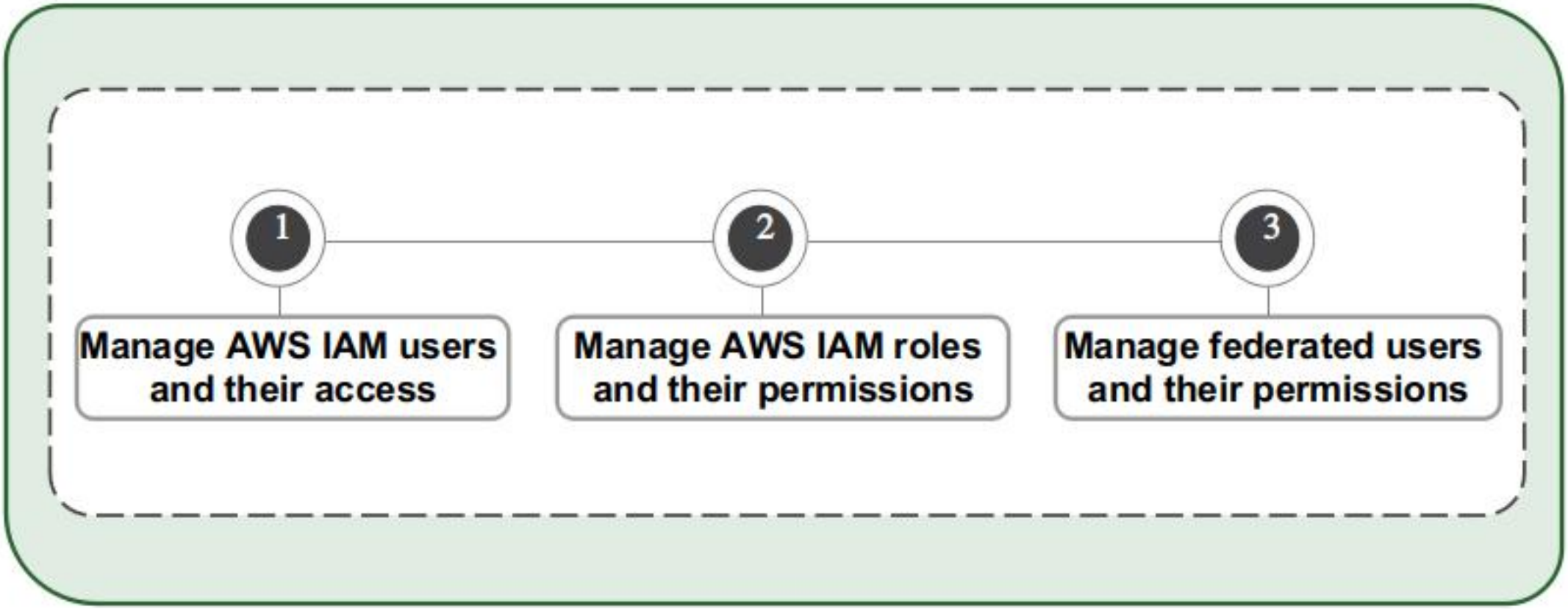
FISMA

- https://aws.amazon.com/compliance/fisma

IAM ACCORDING TO AWS

IAM ACCORDING TO AWS
IAM ACCORDING TO GCP
IAM ACCORDING TO AZURE

AWS IAM



AWS IAM DETAIL

IAM users

- for people

IAM roles

- for computers

IAM Federation

- to federate your workforce into AWS accounts and business applications
- AWS Single Sign-On (SSO) or AWS Identity and Access Management (IAM)

LOGGING IN

(Followed by MFA authentication)

AWS IAM COMMAND-LINE AUTHENTICATION

Authentication

- **AWS CLI or SDK API**
  - Access Key and Secret Key

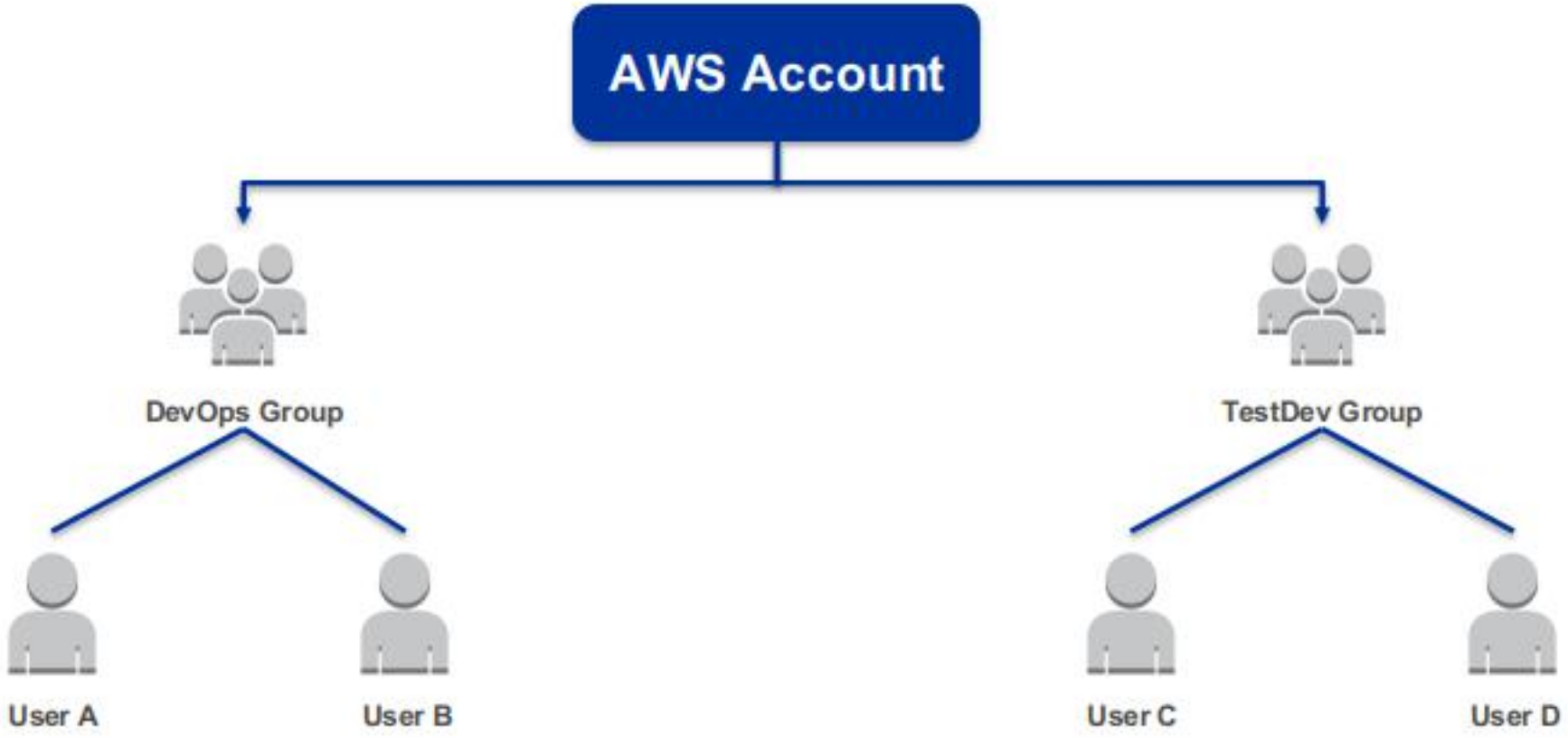
```
Access Key ID: AKIAIOSFODNN7EXAMPLE
Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

AWS CLI

```
[redacted]:~ [redacted]$ aws configure
AWS Access Key ID [****************O22A]:
AWS Secret Access Key [****************4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

AWS SDK & API

AWS IAM USER MANAGEMENT - GROUPS



AWS IAM AUTHORIZATION

Authorization

- Policies:
  - Are JSON documents to describe permissions.
  - Are assigned to Users, Groups or Roles.

IAM User

IAM Group

IAM Roles

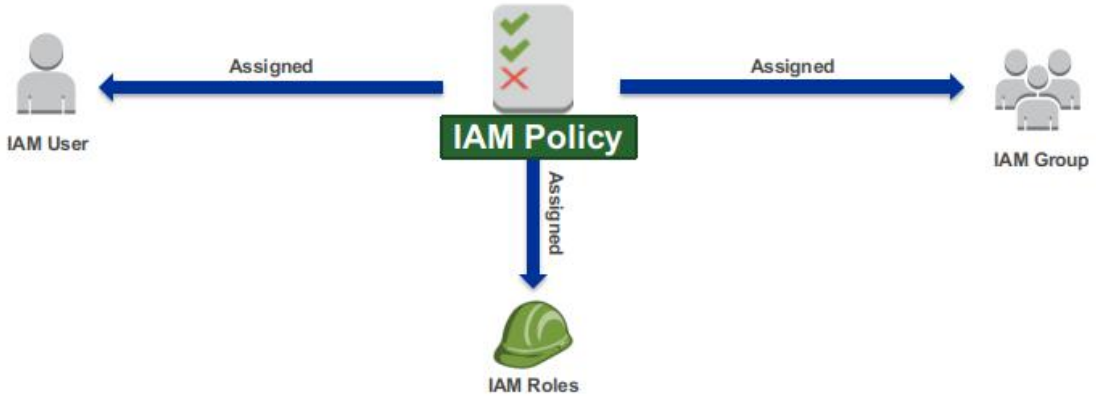
AWS IAM POLICY ELEMENTS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2InstanceConnect",
            "Action": [
                "ec2:DescribeInstances",
                "ec2-instance-connect:SendSSHPublicKey"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS IAM POLICY ASSIGNMENT

These users are bound by the permissions defined in the IAM Policy.

AWS IAM POLICY ASSIGNMENT



IAM Policies may also be assigned to an IAM Role.

An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.

A role is intended to be assumable by anyone who needs it.

Also, a role does not have any credentials (password or access keys) associated with it.

Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

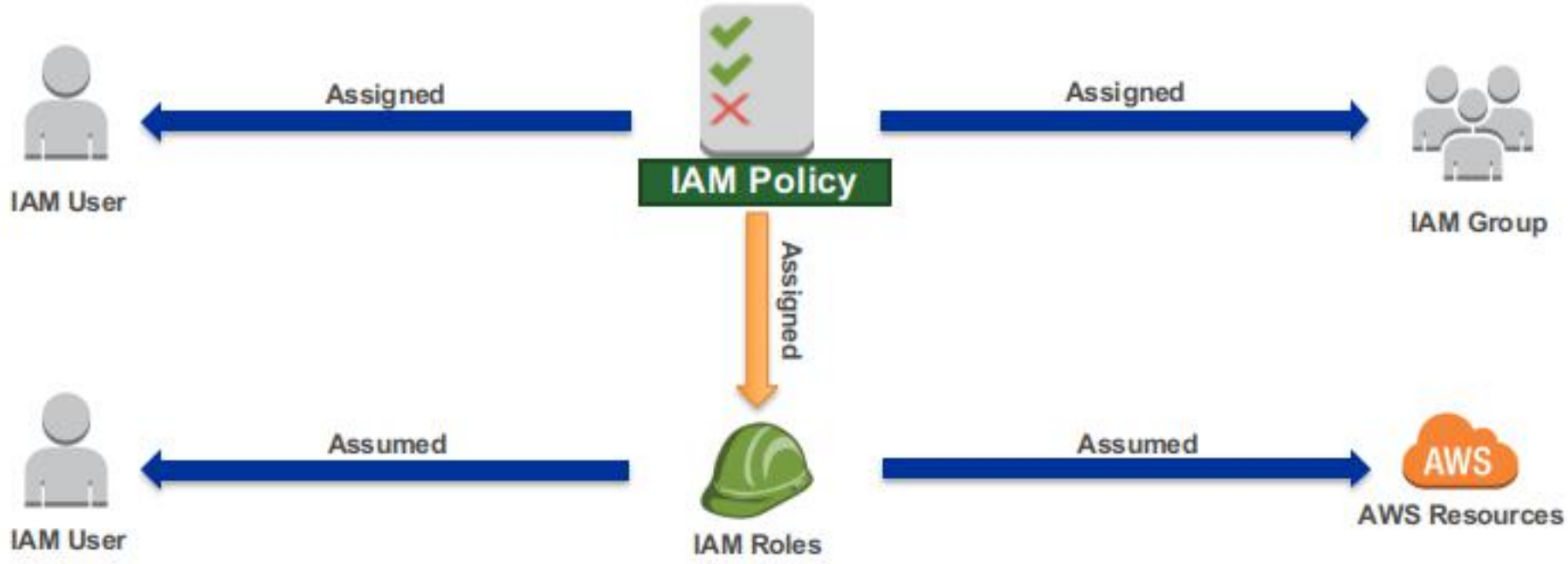
AWS IAM ROLES

An IAM role uses a policy.

An IAM role has no associated credentials.

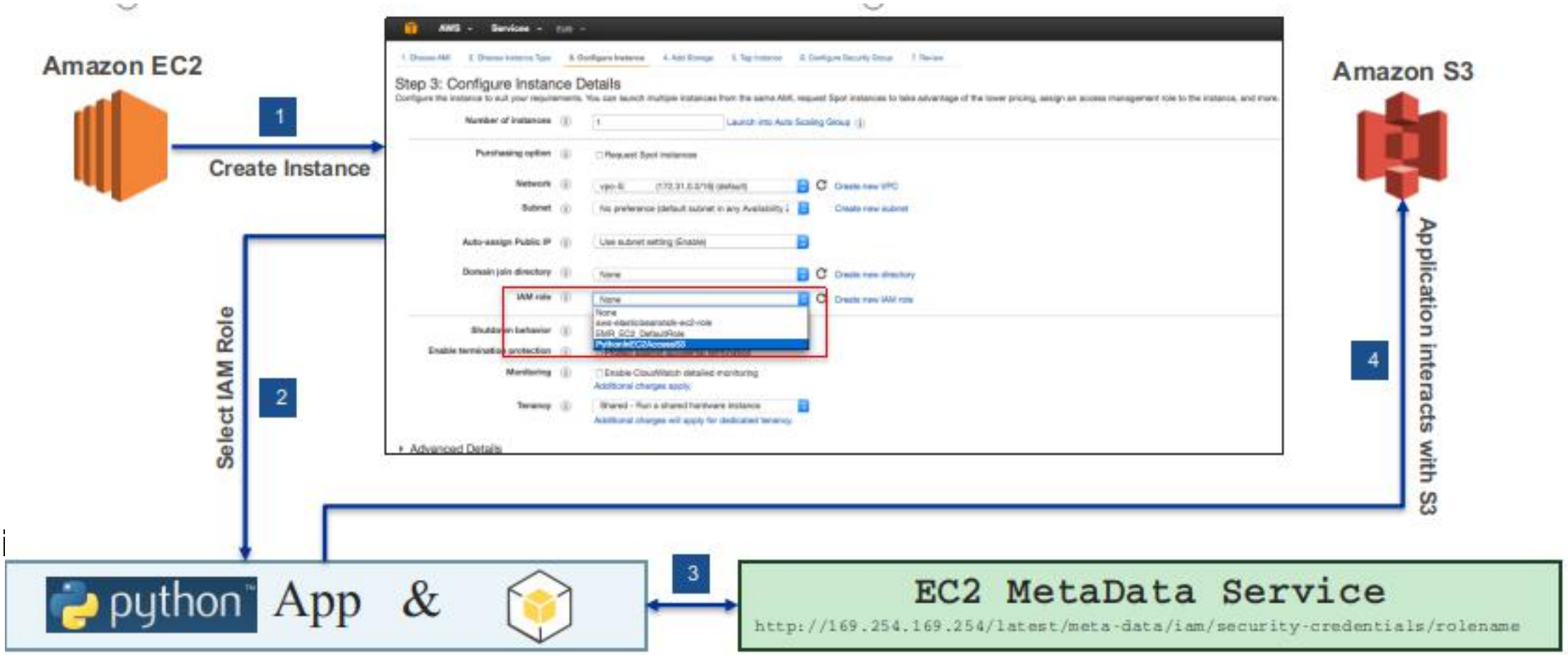
IAM users, applications, and services may assume IAM roles.

AWS IAM POLICY ASSIGNMENT

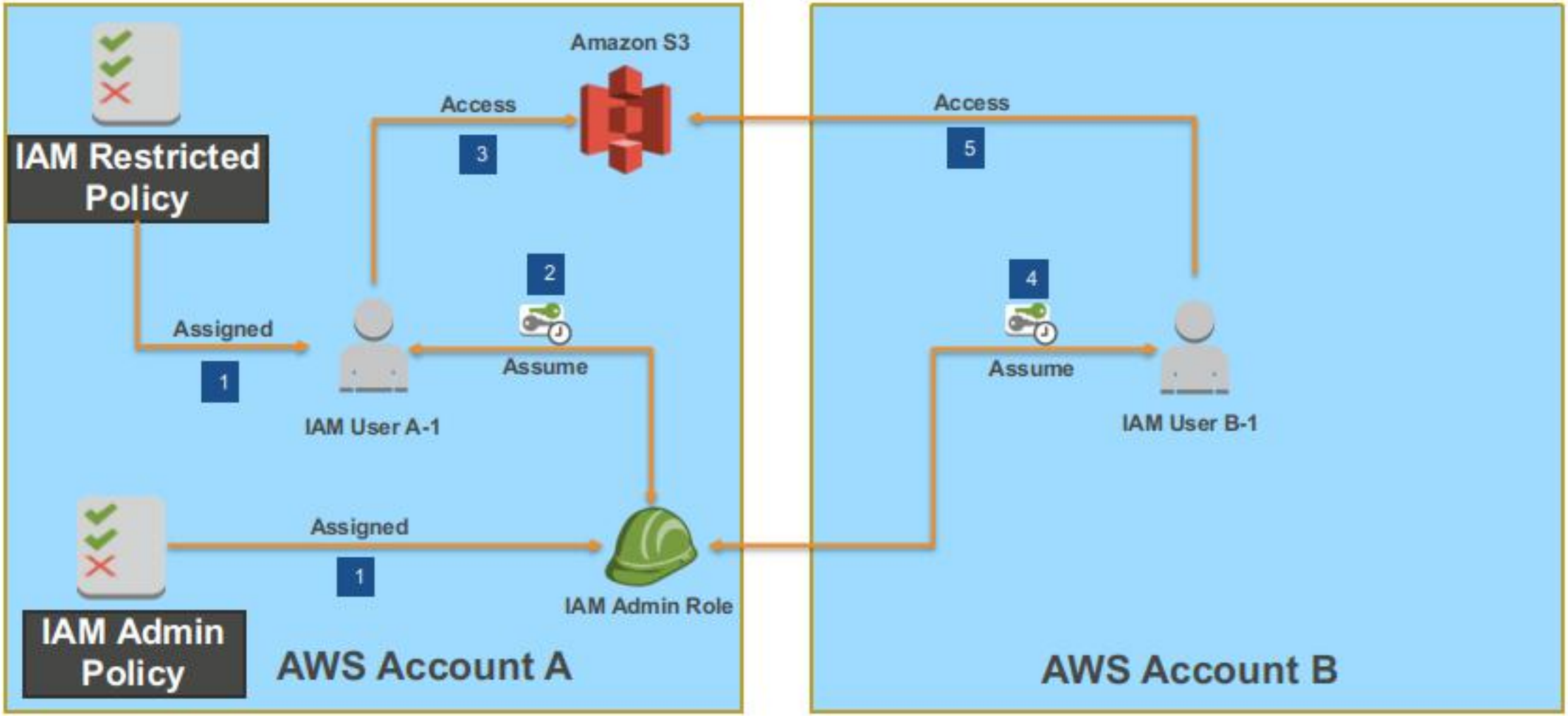


don't

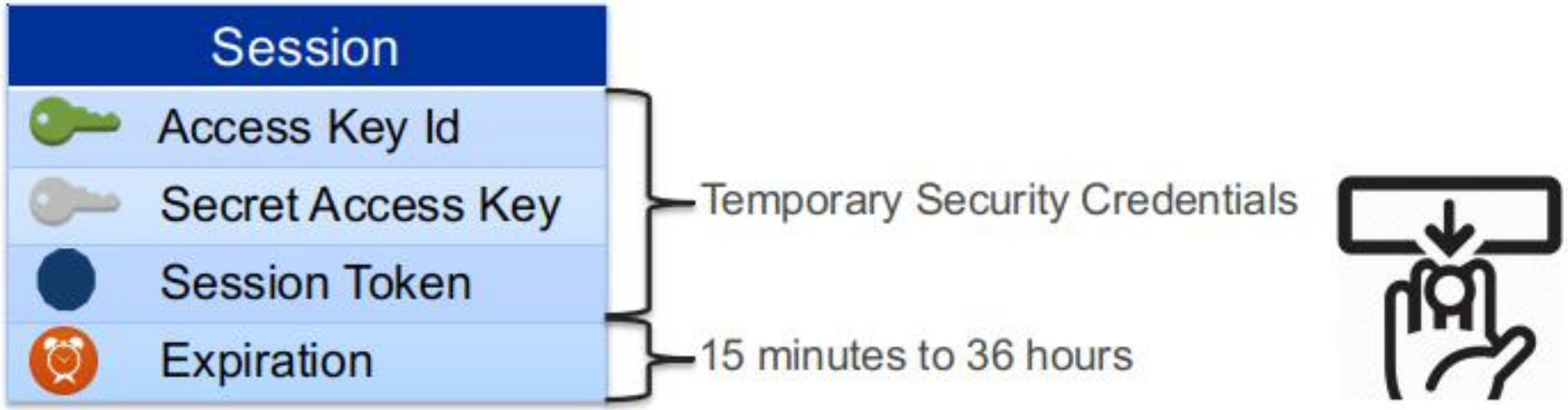
AWS IAM ROLES - INSTANCE PROFILES



AWS IAM ROLES – ASSUME ROLE



TEMPORARY SECURITY CREDENTIALS (AWS STS)



Use Cases

- Cross account access
- Federation
- Mobile Users
- Key rotation for Amazon EC2-based apps

AWS IAM AUTHENTICATION AND AUTHORIZATION

- **Authentication**
  - **AWS Management Console**
    - User Name and Password
  - **AWS CLI or SDK API**
    - Access Key and Secret Key
- **Authorization**
  - Policies

IAM User

IAM Group

IAM Roles

IAM BEST PRACTICES

Delete AWS account (root) access keys.

Create individual IAM users.

Use groups to assign permissions to IAM users.

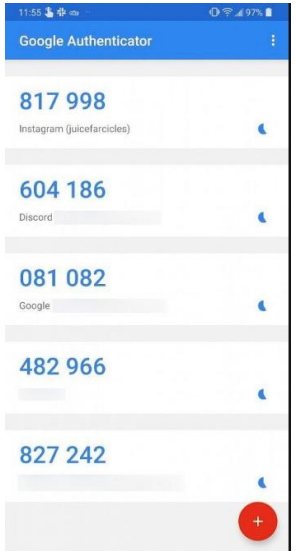
Grant least privilege.

Configure a strong password policy.

Enable MFA for privileged users.

AUTHENTICATOR APPS

Microsoft Authenticator



IAM BEST PRACTICES CONT'D

Use roles for applications that run on cloud instances.

Delegate by using roles instead of by sharing credentials.

Rotate credentials regularly.

Remove unnecessary users and credentials.

Use policy conditions for extra security.

Monitor activity in your cloud account.

QUIZ

Your web application needs to read/write an Amazon DynamoDB table and an Amazon S3 bucket. This operation requires AWS credentials and authorization to use AWS services.

- What service would you use?

QUIZ

Which of the following are managed using IAM (choose 2)

- A) Multi-Factor Authentication
- B) Bucket Policies
- C) Billing Reports
- D) Roles
- E) Security Groups

QUIZ

Which of the following is NOT required as part of AWS's suggested best practices for new accounts?

- A) Delete the root account
- B) Create individual IAM users
- C) Use user groups to assign permissions
- D) Apply an IAM password policy

IAM ACCORDING TO GCP

IAM ACCORDING TO AWS
IAM ACCORDING TO GCP
IAM ACCORDING TO AZURE

GCP RESOURCE MANAGER

Resources in GCP are hierarchically managed by organization, folders, and projects.

Resources Manager enables you to programmatically manage these resource containers.

GCP OBJECTS

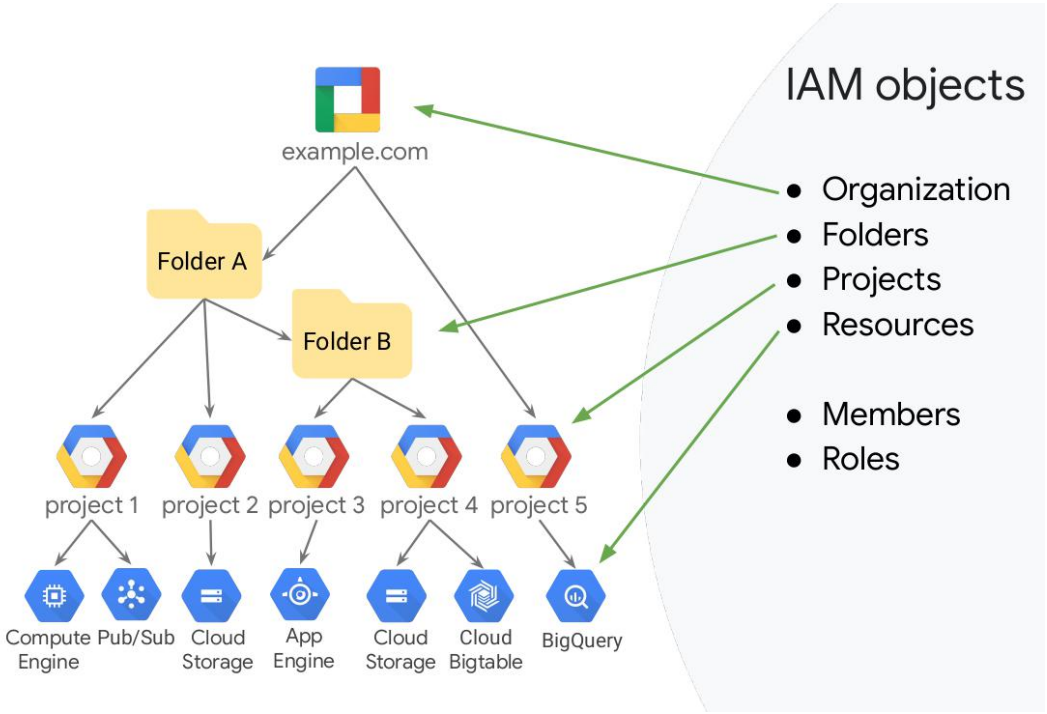
Objects are the various resources members can access and use on GCP.

Objects hold data and applications, and also help to organize it and secure it.

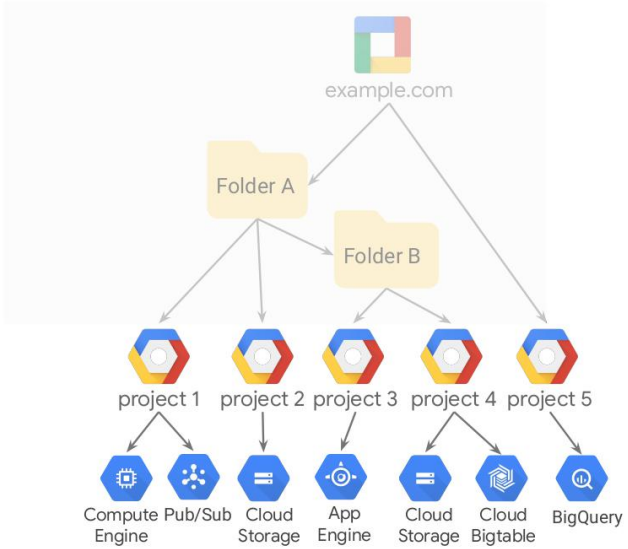
Objects can be

- Organization
- Folders
- Projects
- Resources
- Members
- Roles

GCP OBJECTS



PROJECTS



All GCP resources are associated with a project

- Track resource and quota usage.
- Enable billing.
- Manage permissions and credentials.
- Enable services and APIs.

MEMBERS

Gmail accounts and
Google Groups

Users and groups in
your G Suite domain

Users and groups in your
Cloud Identity domain

You create or manage users or groups outside of GCP

MEMBER ROLES

Member roles are collections of permissions

- Permissions are given to members by granting roles.
- Roles define which permissions are granted.
- GCP provides predefined roles and also the ability to create custom roles.

SERVICE ACCOUNTS

Service accounts:

- Control server-to-server interactions:
- Used to authenticate from one service to another
- Used to control privileges used by resources

Primitive

Predefined

Custom

LABELS IN RESOURCE MANAGER

Labels in Resource Manager help you organize your Google Cloud instances

- Team or cost center labels
- Component labels
- Environment or stage labels
- State labels
- Virtual machine labels

Labels are not designed to hold sensitive information, and doing so may pose

LABS FOR GCP IAM

Cloud IAM: Qwik Start

Service Accounts and Roles: Fundamentals

VPC Network Peering

User Authentication: Identity-Aware Proxy

IAM ROLES IN GCP

Primitive

Predefined

Custom

IAM PRIMITIVE ROLES

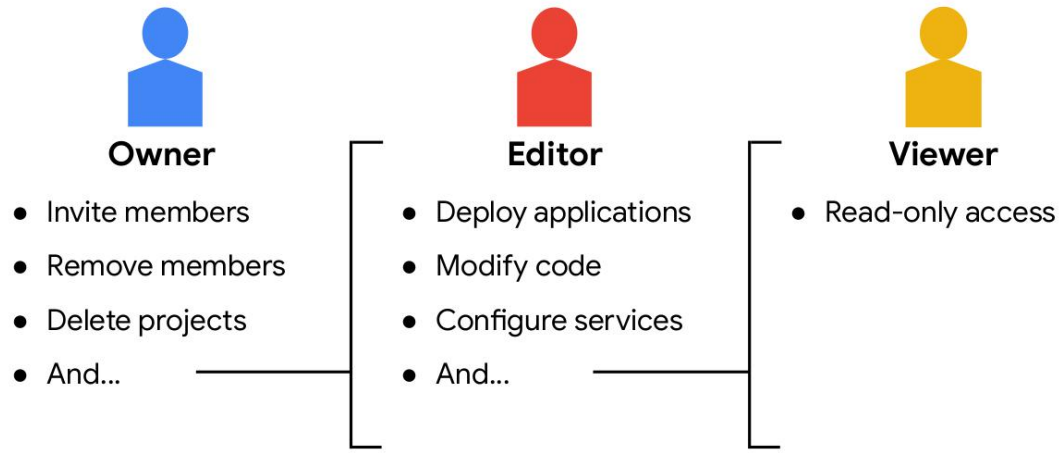
can do what

on **all** resources

IAM primitive roles are applied at the project level

Primitive roles offer fixed, coarse-grained levels of access

IAM PRIMITIVE ROLES



Primitive roles apply across all GCP services in a project

IAM PREDEFINED ROLES

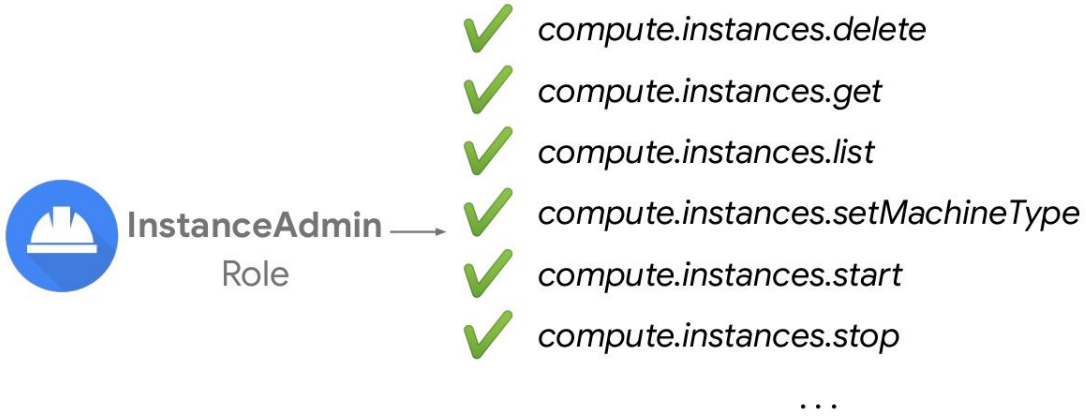
Predefined roles are designed to map to job functions: Compute Network Admin, Security Reviewer, etc.

Predefined roles provide granular access for a specific service. They are designed to map to job functions, for example, Compute Network Admin, Security Reviewer, Storage Admin, etc.

Predefined roles are managed by Google Cloud. So if a new feature or service is added in the future, the appropriate permissions will be added to any predefined role that requires them.

IAM PREDEFINED ROLES ARE MORE FINE-GRAINED

IAM predefined roles offer more fine-grained permissions on particular services



SYSTEM EVENT AUDIT LOGS

System event audit logs record activity that modifies the configuration of your resources

- Driven by Google system events
- Not triggered by user interaction
- Always written and cannot be disabled

IAM POLICIES

A Cloud IAM policy is used to specify access control policies for Google Cloud resources.

A policy consists of a list of bindings

A binding binds a list of members to a role

RESOURCE POLICIES ARE A UNION

resource policies are a union of parent and resource

a less restrictive parent policy will always override a more restrictive resource policy.

IAM RECOMMENDER

The Cloud IAM recommender helps you enforce the principle of least privilege by ensuring that members have only the permissions that they actually need

- Recommender compares project-level role grants with permissions used within the last 90 days
- If a permission has not been used within that time, recommender will suggest revoking it
- You have to review and apply recommendations; they will not be applied automatically

THREE TYPES OF RECOMMENDATIONS

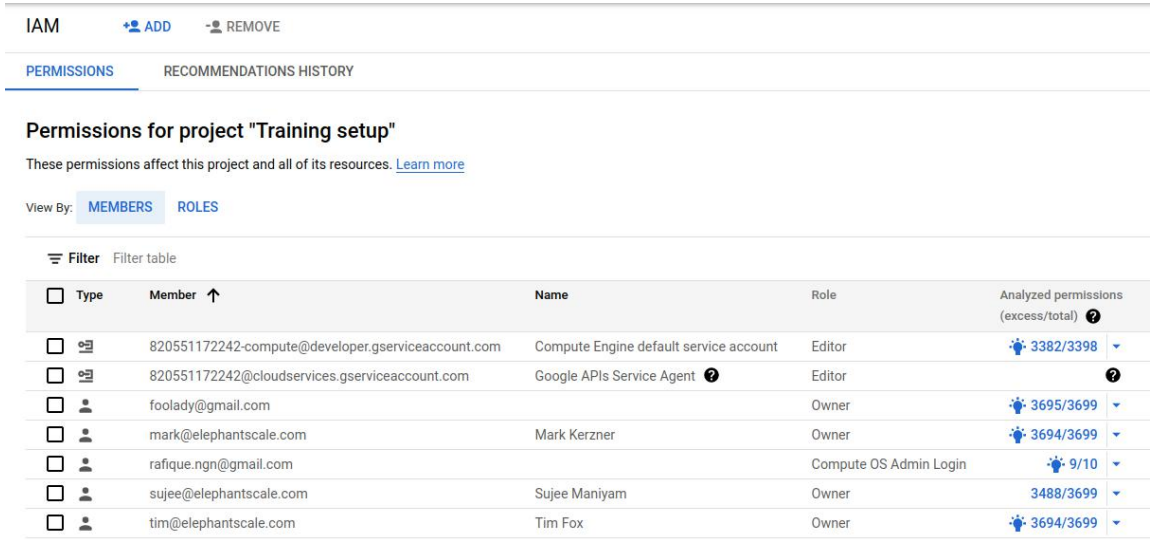
Recommender gives you three types of recommendations

- Revoke an existing role
- Replace an existing role
- Add permissions to an existing role

APPLY RECOMMENDER

View existing roles by visiting the IAM page

- Look for the “over-granted permissions” column
- If there are recommendations, you will see a Recommendation available icon
- Click the Recommendation available icon for details
- Choose to “apply” or to “dismiss” a recommendation
- You can revert your choice within 90 days



IAM AUDIT LOGS

Cloud Audit Logs maintains three logs for each project, folder and organization

- Admin activity audit logs
- Data access audit logs
- System event audit logs

To view

- Basic log viewer
- Advanced log viewer
- gcloud command-line tool
- Audit Logs API

IAM BEST PRACTICES

Adhere to the Principle of Least Privilege, which means you should always apply only the minimal access level required to get the job done

IAM BEST PRACTICES

Use groups when configuring GCP access

Assign roles to the groups instead of individual users

Utilizing predefined roles offers less administrative overhead

Predefined roles are managed by Google

Custom roles are not maintained by Google

IAM BEST PRACTICES

Audit logs record project-level permission changes

Audit policy changes

Export audit logs

Explore audit logs to Cloud Storage to store your logs for long periods of time

QUIZ

Which FOUR of the following are Cloud IAM Objects that can be used to organize resources in GCP?

A) Bucket

B) Folder

C) Role

D) Member

E) Instance

F) Container

G) Organization

QUIZ

In Google Cloud IAM, if a policy gives you Owner permissions at the project level, your access to an individual resource in the project may be restricted to View by applying a more restrictive policy to that resource.

A) True

B) False

QUIZ

All Google Cloud Platform resources are associated with a project.

A) True

B) False

QUIZ

What is the difference between IAM primitive roles and IAM predefined roles?

A) Primitive roles affect all resources in a GCP project, but predefined roles apply to a particular service in a project

B) Primitive roles apply to a particular service in a project, but predefined roles affect all resources in a GCP project

C) Neither

IAM ACCORDING TO AZURE

IAM ACCORDING TO AWS
IAM ACCORDING TO GCP
IAM ACCORDING TO AZURE

AZURE AD

Azure Active Directory (Azure AD)

User's account

- type of user
- role assignments
- ownership of individual objects.

AZURE ACCOUNT TYPES

Administrators

- The highest level of access

Member user accounts

- in the Azure AD organization

Guest users

- the most restricted level of access.

PERMISSIONS AND ROLES

Azure AD uses permissions to help you control the access rights a user or group is granted

This is done through roles.

Azure AD has many roles with different permissions attached to them.

When a user is assigned a specific role, they inherit permissions from that role.

- For example, a user assigned to the User Administrator role can create and delete user accounts.

ADMINISTRATOR ROLES

Elevated access to control who is allowed to do what.

Assigned to a limited group of users to manage identity tasks in an Azure AD organization.

For User Administrator or Global Administrator role

- you can create a new user in Azure AD by using either the Azure portal
- the Azure CLI `az ad user create`
- or PowerShell `cmdlet New-AzureADUser`

MEMBER USERS

A native member of the Azure AD organization

- has a set of default permissions like being able to manage their profile information.
- New users typically have this type of account created for them.
- for users who are considered internal to an organization and are members of the Azure AD organization. However, these users shouldn't be able to manage other users by, for example, creating and deleting users

GUEST USERS

Have restricted Azure AD organization permissions

Invited to collaborate with your organization

- Either send an invitation email that contains a redemption link or
- send a direct link to an app you want to share.
- Guest users sign in with their own work, school, or social identities.

Azure AD member users can invite guest users

This default can be disabled by someone who has the User Administrator role.

ADD USER ACCOUNTS

Azure

```
# create a new user
az ad user create
```

```
# create a new user
New-AzureADUser
```

BULK CREATE MEMBERS

PowerShell

```
$invitations = import-csv c:\bulkinvite\invitations.csv

$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo

$messageInfo.customizedMessageBody = "Hello. You are invited to the Contoso organization."

foreach ($email in $invitations)
   {New-AzureADMSInvitation `
      -InvitedUserEmailAddress $email.InvitedUserEmailAddress `
      -InvitedUserDisplayName $email.Name `
      -InviteRedirectUrl https://myapps.microsoft.com `
      -InvitedUserMessageInfo $messageInfo `
      -SendInvitationMessage $true
   }
```

DELETE USER ACCOUNTS

Azure

```
# delete a user
az ad user delete.
```

```
# delete a user
Remove-AzureADUser
```

QUIZ

If you delete a user account by mistake, can it be restored?

- A) When a user account is deleted, it's gone forever and can't be restored.
- B) The user account can be restored, but only when it's created within the last 30 days.
- C) The user account can be restored, but only when it's deleted within the last 30 days.

QUIZ

What kind of account would you create to allow an external organization easy access?

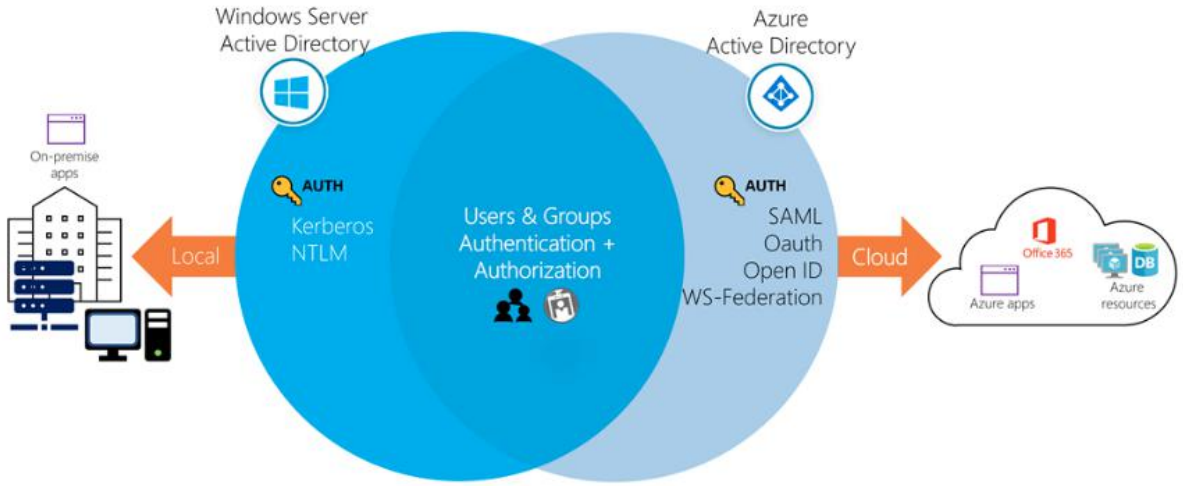
- A) A guest user account for each member of the external team.
- B) An external account for each member of the external team.
- C) An administrator account for each member of the external team.

AZURE AD IS NOT WINDOWS SERVER AD

Azure AD not intended as a complete replacement for an on-premises Active Directory

If you're already using a Windows AD server, you can connect it to Azure AD to extend your directory into Azure

You can use the same credentials to access local and cloud-based resources.



DIRECTORIES, SUBSCRIPTIONS, AND USERS

All these subscriptions can use Azure AD

- Microsoft Azure
- Microsoft 365
- Microsoft Intune
- Microsoft Dynamics 365

Subscriptions in Azure are both

- billing entity
- security boundary

DIRECTORIES, SUBSCRIPTIONS, AND USERS

A subscription is associated with a single Azure AD directory.

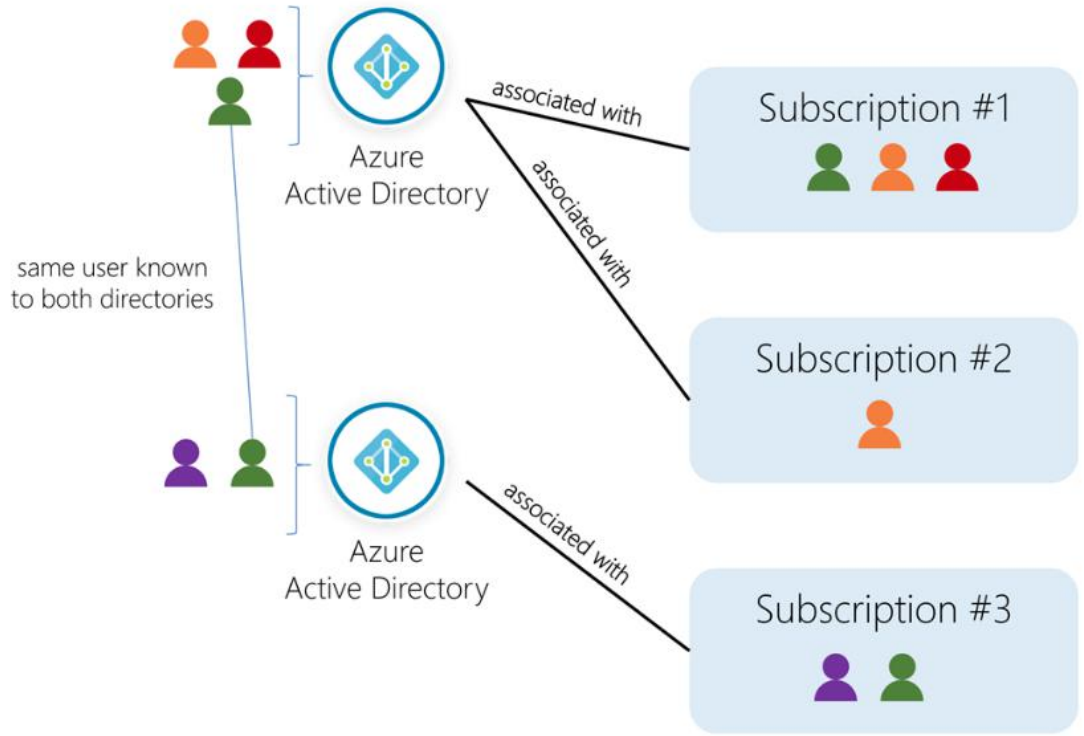
Multiple subscriptions can trust the same directory, but a subscription can only trust one directory.

Users and groups can be added to multiple subscriptions

- the user can create, control, and access resources in the subscription.

The user in a subscription must be known to the associated directory as shown in the following image.

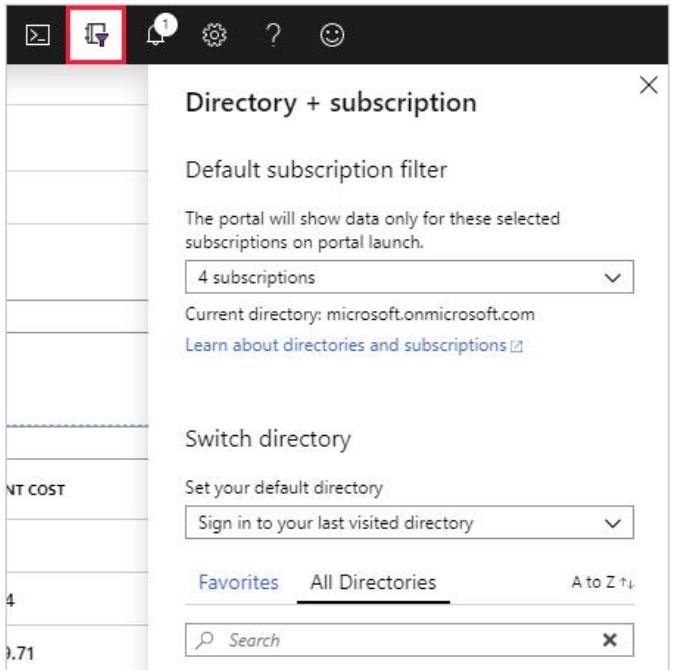
DIRECTORIES, SUBSCRIPTIONS, AND USERS



SWITCHING DIRECTORY

If you belong to multiple directories

- you can switch the current directory
- through the Directory + subscription button in the Azure portal header.



QUIZ

An Azure subscription is a _____.

- A) billing entity and security boundary
- B) container that holds users
- C) monthly charge for Azure services

QUIZ

Which of the following best describes the relationship between a subscription and an Azure AD directory?

- A) An Azure AD directory has a 1:1 relationship with a subscription.
- B) An Azure AD directory can be associated with multiple subscriptions, but a subscription is always tied to a single directory.
- C) An Azure AD directory is associated with a single subscription, but a subscription can trust multiple directories.

QUIZ

A organization can have more than one Azure AD directory.

- A) True
- B) False

BUILT-IN ROLES FOR AZURE RESOURCES

Owner

- has full access to all resources, including the right to delegate access to others.

Contributor

- can create and manage all types of Azure resources but can’t grant access to others.

Reader

- can view existing Azure resources.

ROLE DEFINITIONS

A set of properties defined in a JavaScript Object Notation (JSON) file

Try this

```
1 Get-AzureRmRoleDefinition -Name Owner
```

You will get this

```
1 Name             : Owner
2 Id               : 8e3af657-a8ff-443c-a75c-2fe8c4bcb635
3 IsCustom         : False
4 Description      : Lets you manage everything, including access to resources.
5 Actions          : {*}
6 NotActions       : {}
7 DataActions      : {}
8 NotDataActions   : {}
9 AssignableScopes : {/}
```

RBAC: ROLE-BASED ACCESS CONTROL

Contributor role definition in JSON format

```
{
  "Name": "Contributor",
  "Id": "b24988ac-6180-42a0-ab88-20f7382dd24c",
  "IsCustom": false,
  "Description": "Lets you manage everything except access to resources.",
  "Actions": [
    "*"
  ],
  "NotActions": [
    "Microsoft.Authorization/*/Delete",
    "Microsoft.Authorization/*/Write",
    "Microsoft.Authorization/elevateAccess/Action"
  ],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

DISCUSSION

Let us describe some patterns for roles and policies for a typical research lab

CONGRATS ON COMPLETION