www.eazytraining.fr

Services de sécurité & gestion de compte

Par Lahda Biassou Alphonsine

Lahda Biassou Alphonsine

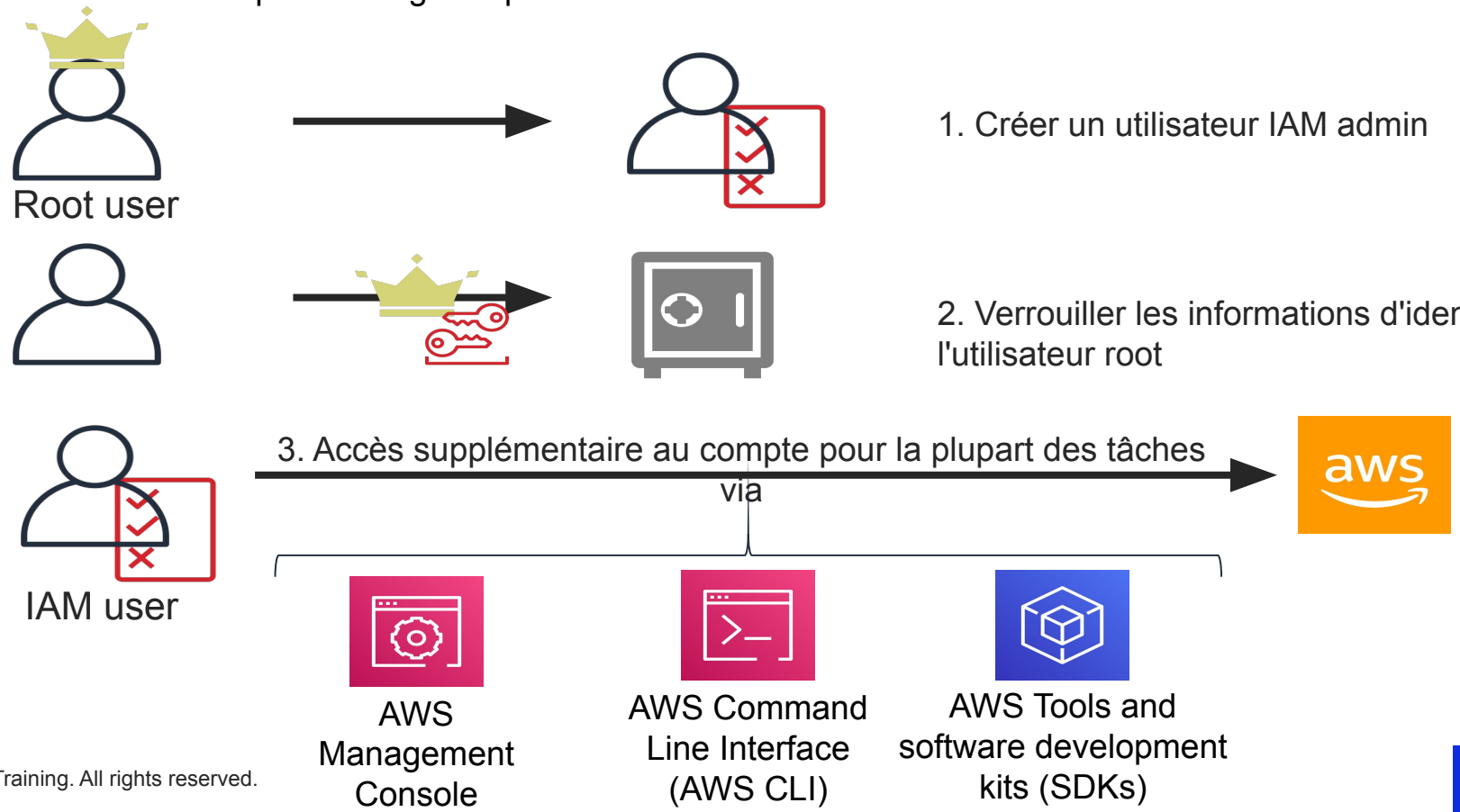
Ingénieure cloud et formatrice

Plan

- **Compte utilisateur et IAM**
- **Organiser les utilisateurs**
- **Fédérer les utilisateurs**
- **Comptes multiples**

Compte utilisateur & IAM - Sécuriser le compte root

Le compte de l'utilisateur root dispose d'un grand pouvoir. Mesures de sécurité recommandées :



AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)

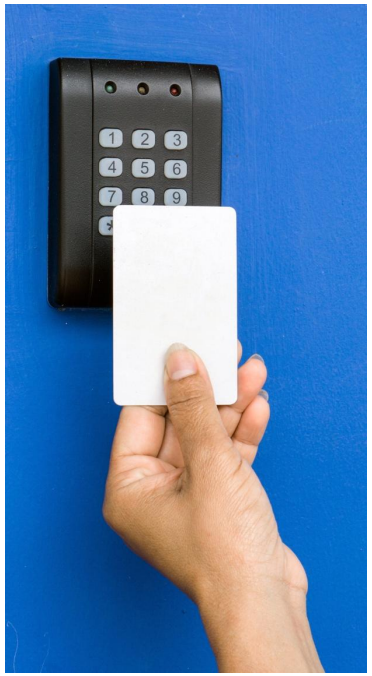
Contrôlez en toute sécurité l'accès individuel et collectif à vos ressources AWS.

Intégration avec d'autres services AWS

Gestion des identités fédérées

Permissions granulaires

Prise en charge de l'authentification multifactorielle



Composants IAM : Examen

IAM user

Défini dans votre compte AWS. Utilisez les informations d'identification pour vous authentifier par programme ou via la console de gestion AWS.

IAM group

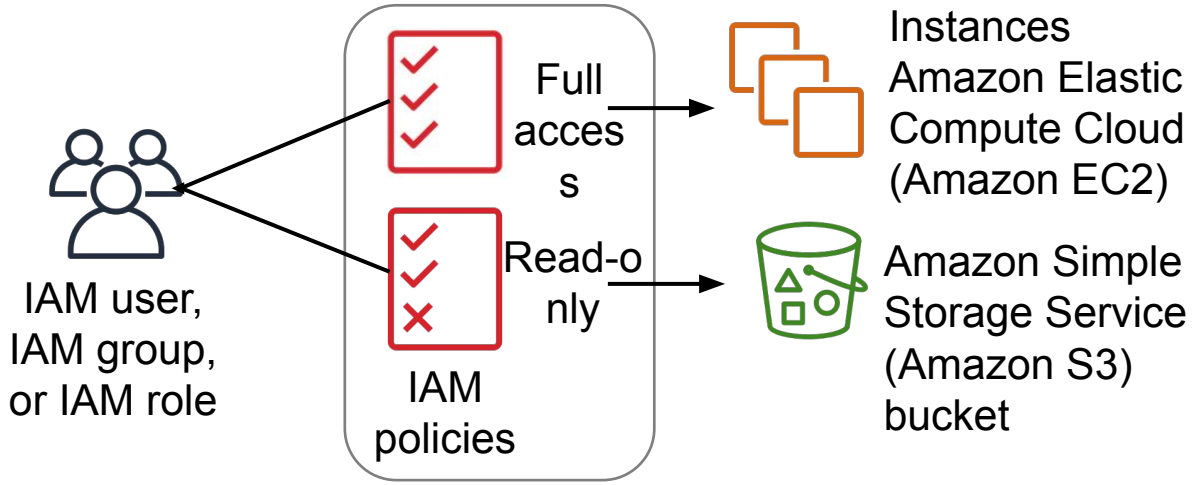
Ensemble d'utilisateurs IAM bénéficiant d'une autorisation identique.

IAM policy

Définit les ressources auxquelles il est possible d'accéder et le niveau d'accès à chaque ressource.

IAM role

Mécanisme permettant d'accorder un accès temporaire pour effectuer des demandes de services AWS. Assumable par une personne, une application ou un service.



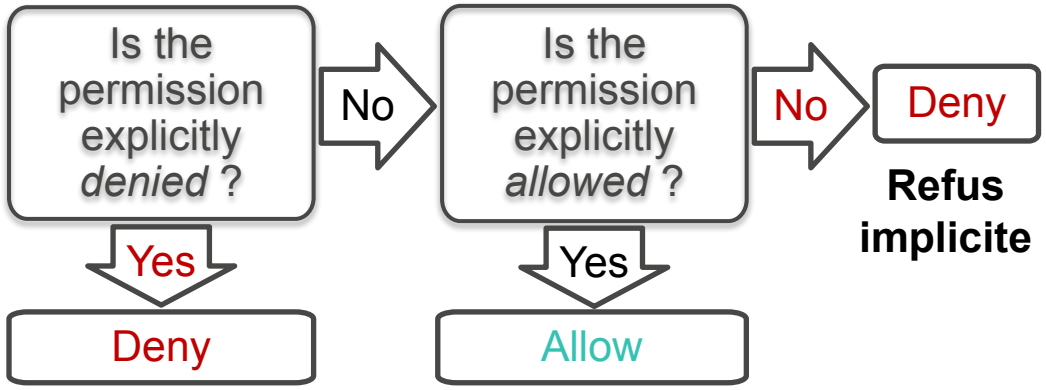
Les permissions IAM

Politique IAM

Les autorisations sont spécifiées dans une politique IAM :

- Document formaté en notation d'objets JavaScript (JSON).
- Il définit les ressources et les opérations autorisées
- Meilleure pratique - suivre le principe du moindre privilège
- Deux types de politiques
  - Basées sur l'identité : attachées à un principal IAM
  - Basées sur les ressources : attachées à une ressource AWS.

Comment l'IAM détermine les autorisations au moment de la demande :



Politiques basées sur l'identité ou sur les ressources

Politiques basées sur l'identité

- Attached to a user, group, or role
- Types of policies
  - AWS managed
  - Customer managed
  - Inline

Politiques basées sur les ressources

- Attached to AWS resources
  - Example: Attach to an Amazon S3 bucket
- Always an inline policy

Structure du document de politique IAM

```
{
   "Version": "2012-10-17",
   "Statement":[{
      "Effect": "effect",
      "Action": "action",
      "Resource": "arn",
      "Condition":{
         "condition":{
            "key": "value"
         }
      }
   }]
}
```

- Effect: l'effet peut être *Allow* or *Deny*
- Action: type d'accès qui est allowed or denied

```
"Action": "s3:GetObject"
```

- Resource: Ressources sur lesquelles l'action agira

```
"Resource": "arn:aws:sqs:us-west-2:123456789012:queue1"
```

- **Condition**: Conditions à remplir pour que la règle s'applique

```
"Condition" : {
    "StringEquals" : {
        "aws:username" : "johndoe"
    }
}
```

ARN et caractères génériques

- Resources are identified by using Amazon Resource Name (ARN) format
  - Syntax – `arn:`*`partition`*`:`*`service`*`:`*`region`*`:`*`account`*`:`*`resource`*
  - Example – `"Resource": "arn:aws:iam::123456789012:user/mmajor"`

- You can use a wildcard (*) to give access to all actions for a specific AWS service
  - Examples –
    - `"Action": "s3:*"`
    - `"Action": "iam:*AccessKey*"`

Exemple de politique d'AM

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:* ","s3:*"],
    "Resource":[
      "arn:aws:dynamodb :region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Explicit allow permet aux utilisateurs d'accéder à une table DynamoDB spécifique et...

...Amazon S3 buckets.

Explicit deny garantit que les utilisateurs ne peuvent pas utiliser d'autres actions ou ressources AWS que cette table et ces buckets.

Une déclaration de refus explicite **takes precedence** sur une déclaration d'autorisation.

Activité : Analyse de la politique d'AIM

```
{
  "Version": "2012-10-17",
  "Statement":[{
      "Condition": {
        "StringNotEquals": {
           "ec2:InstanceType": [
              "t2.micro",
              "t2.small"
           ]
        }
      },
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Action": [
         "ec2:RunInstances",
         "ec2:StartInstances"
      ],
     "Effect": "Deny"
}
```

- Quelles actions la politique autorise-t-elle ?

RÉPONSE : Elle ne vous autorise à rien (l'effet est de refuser).

- Supposons que la politique comprenne un objet de déclaration supplémentaire, comme dans l'exemple suivant :

{

« Effet » : « Autoriser »,
« Action » : « ec2:* »

}

- Comment la politique limiterait-elle l'accès qui vous est accordé par cette déclaration supplémentaire ?

RÉPONSE : Vous aurez un accès complet au service Amazon EC2. Cependant, vous ne seriez autorisé qu'à lancer ou démarrer des instances EC2 de type t2.micro ou t2.small.

- Si la politique incluait à la fois la déclaration de gauche et la déclaration de la question pourriez-vous mettre fin à une instance m3.xlarge qui existait sur le compte ?

RÉPONSE : Oui.

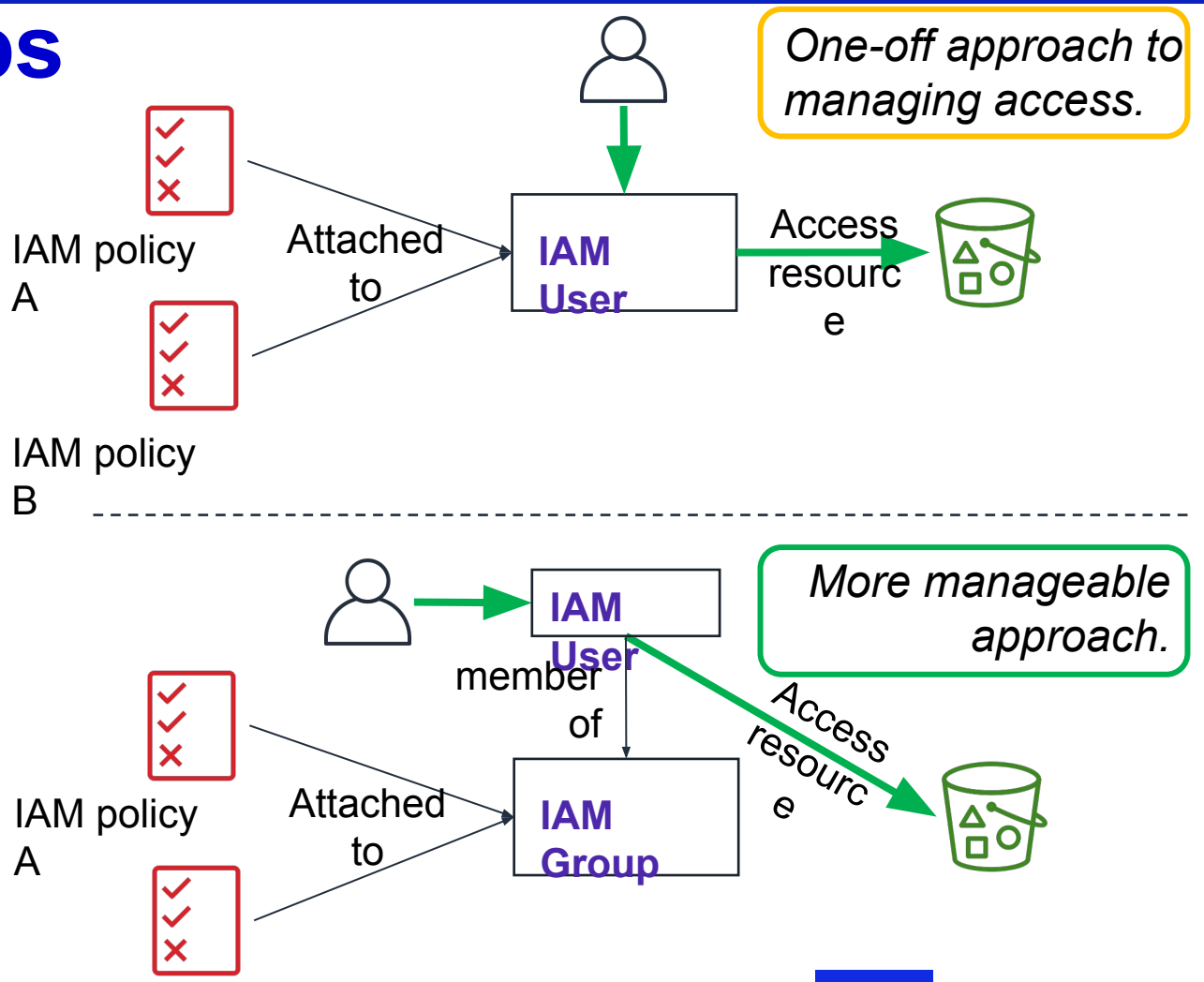
IAM groups

Les groupes IAM permettent d'accorder les mêmes droits d'accès à plusieurs utilisateurs.

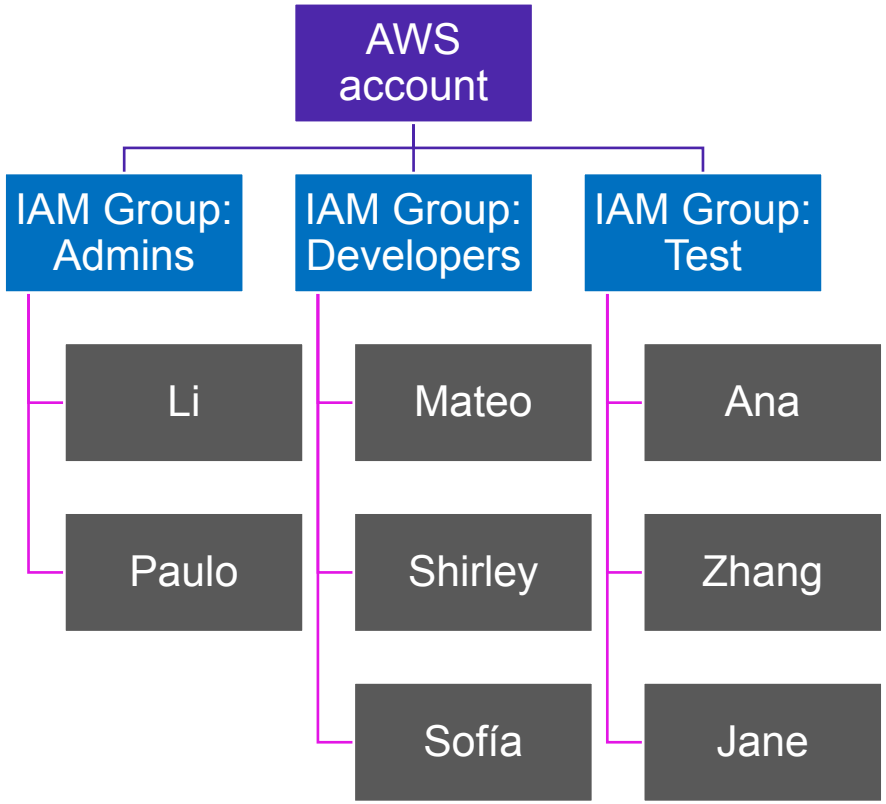
- Tous les utilisateurs du groupe héritent des autorisations attribuées au groupe.
- Facilite la gestion de l'accès pour plusieurs utilisateurs.

Conseil : Combiner les approches pour un accès individuel précis

- Ajoutez l'utilisateur à un groupe pour appliquer un accès standard basé sur la fonction.
- Attachez éventuellement une politique supplémentaire à l'utilisateur pour les exceptions nécessaires.



Exemples de groupes IAM



Conseil : Créez des groupes qui reflètent les fonctions du poste

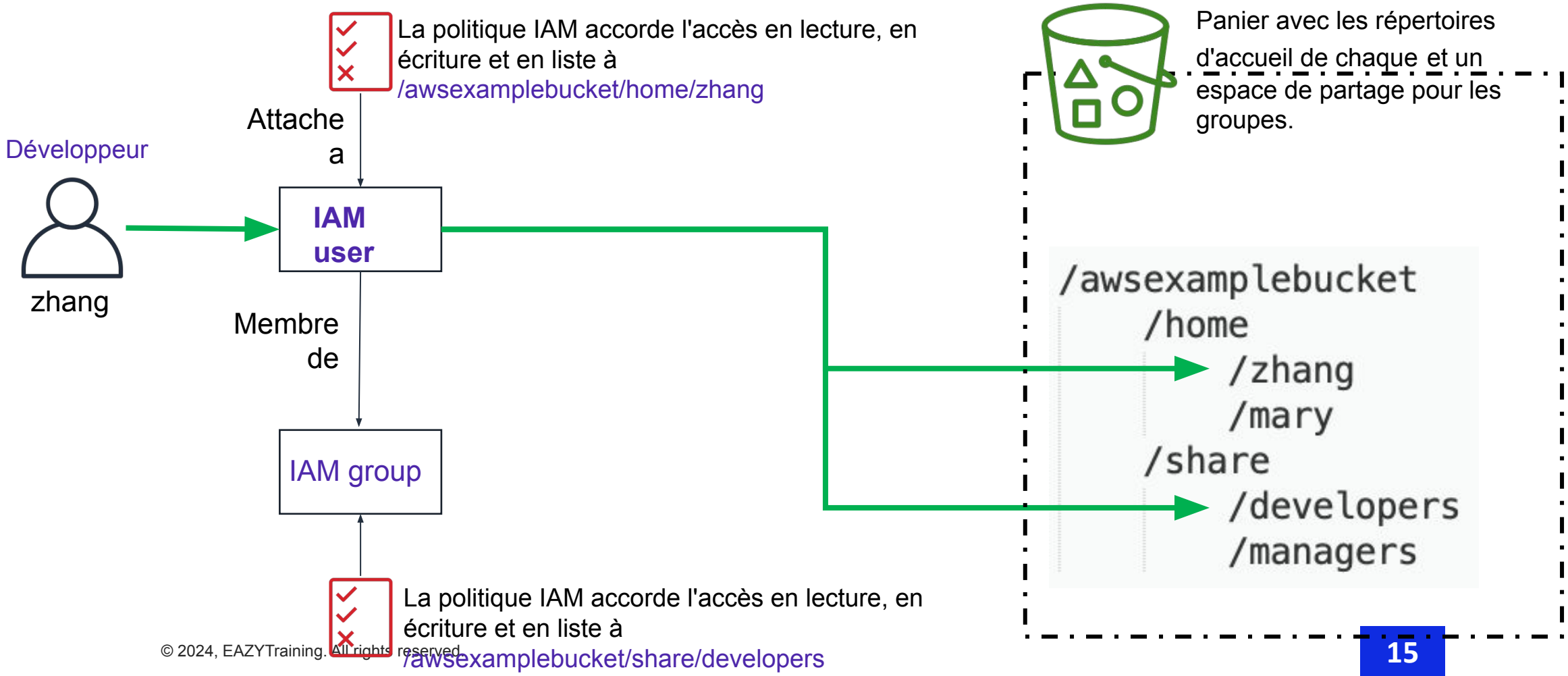
- Si un nouveau développeur est embauché, ajoutez-le au groupe Développeur.
- Il hérite immédiatement du même accès que les autres développeurs.

- Si Ana prend le rôle de développeur -
  - Retirez-la du groupe Test
  - L'ajouter au groupe Développeurs

- Les utilisateurs peuvent appartenir à plusieurs groupes

Toutefois, c'est la politique la plus restrictive qui s'applique

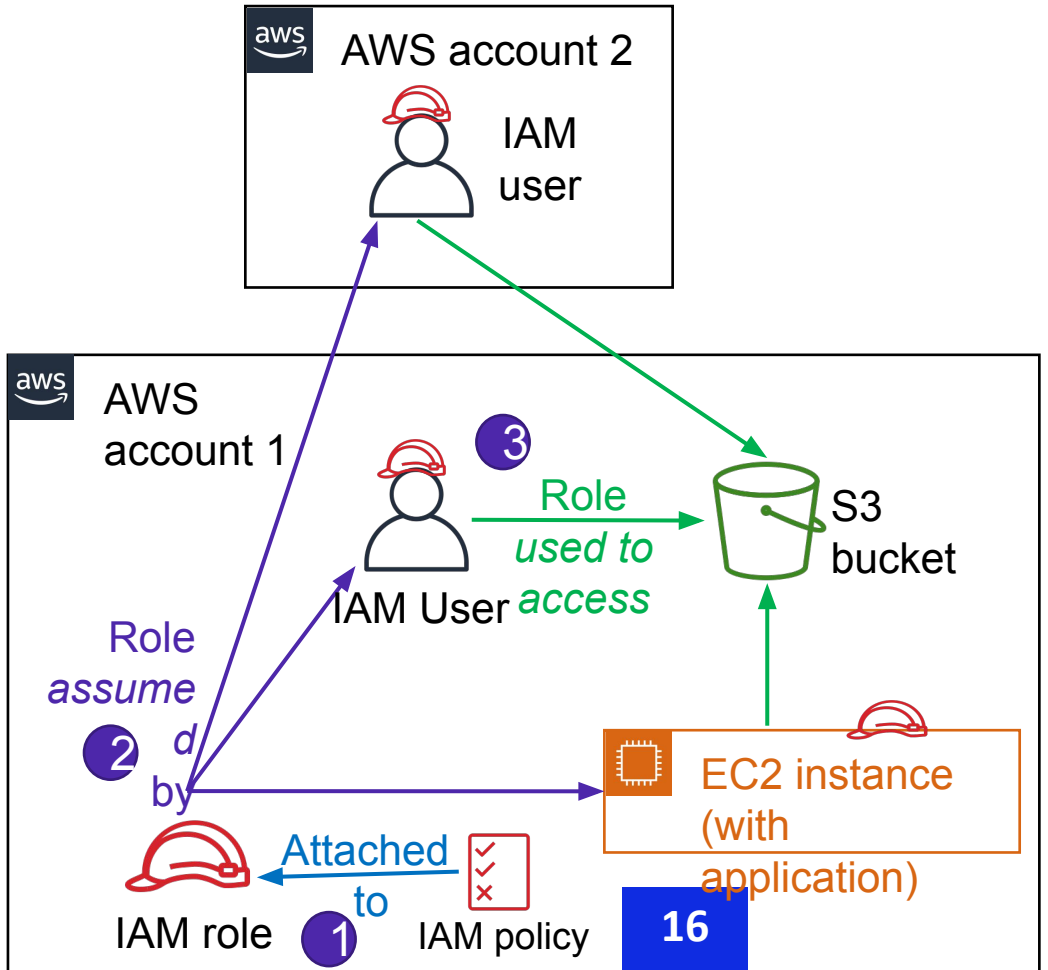
Cas d'utilisation de l'IAM avec Amazon S3



Fédération d'utilisateur -Rôles IAM

- Caractéristiques du rôle IAM
  - Fournit des informations d'identification de sécurité temporaires
  - n'est pas associé de manière unique à une personne
- Peut être assumé par une personne, une application ou un service
  - Est souvent utilisé pour déléguer l'accès

- Cas d'utilisation
  - Fournir aux ressources AWS un accès aux services AWS
  - Fournir un accès à des utilisateurs authentifiés en externe
  - Fournir un accès à des tiers
  - Changer de rôle pour accéder aux ressources dans -
    - votre compte AWS
    - Tout autre compte AWS (accès croisé)



Accorder des autorisations pour assumer un rôle

AWS Security Token Service (AWS STS)

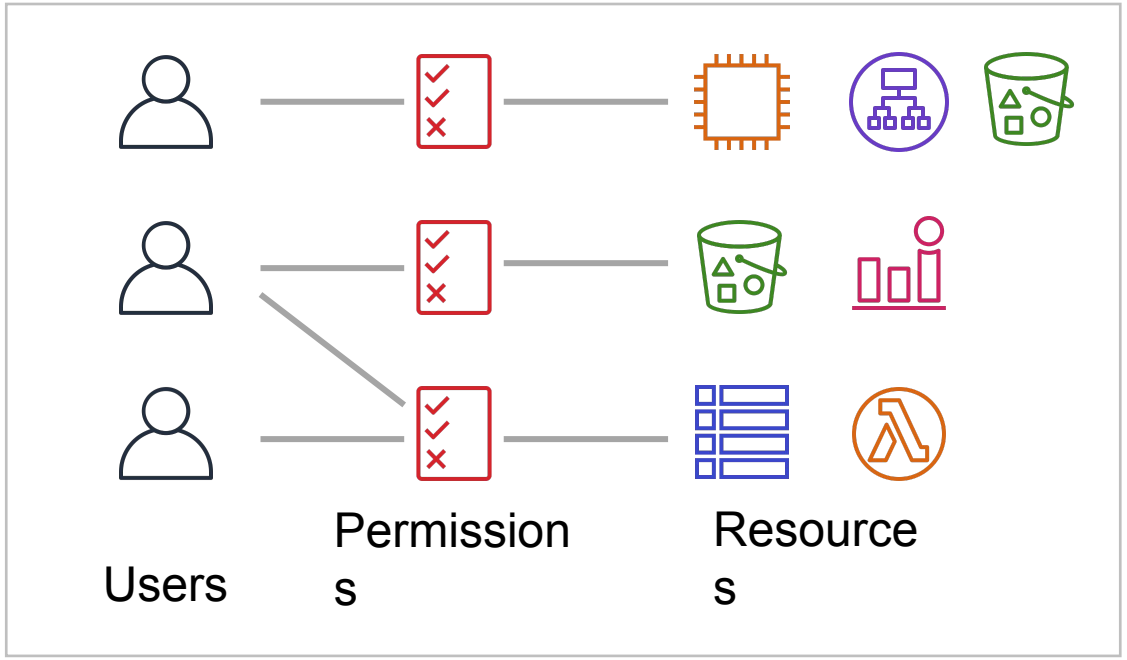
- Pour qu'un utilisateur IAM, une application ou un service puisse assumer un rôle, vous devez lui accorder des autorisations de passage au rôle.
- Service de jetons de sécurité AWS (AWS STS)
  - Service web qui vous permet de demander des informations d'identification temporaires à privilèges limités.
  - Les informations d'identification peuvent être utilisées par les utilisateurs IAM ou par les utilisateurs que vous authentifiez (utilisateurs fédérés).
- Exemple de politique - Permet à un utilisateur IAM d'assumer un rôle

```
{
   "Version": "2012-10-17",
   "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole ",
    "Resource": "arn:aws:iam::123456789012:role/Test*"
   }
}
```

Role-based access control (RBAC)

Approche traditionnelle du contrôle d'accès :

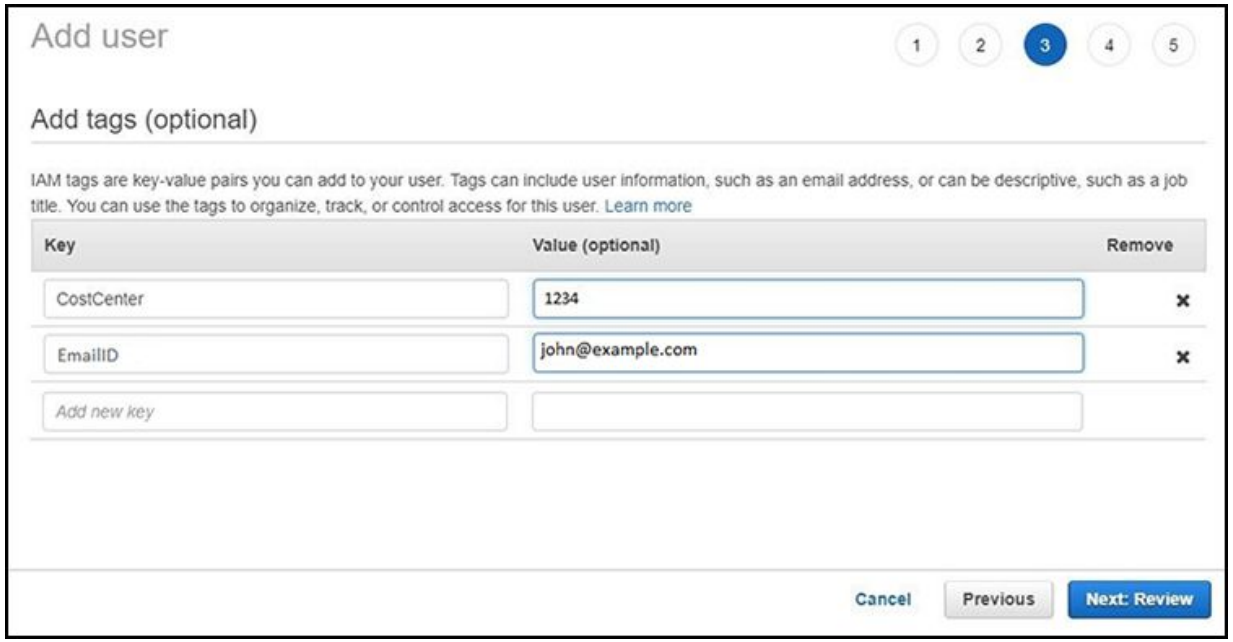
- Accorder aux utilisateurs des autorisations spécifiques basées sur leur fonction (par exemple, administrateur de base de données).
- Créer un rôle IAM distinct pour chaque combinaison d'autorisations.
- Mettre à jour les autorisations en ajoutant un accès pour chaque nouvelle ressource (la mise à jour permanente des politiques peut s'avérer fastidieuse).



Meilleure pratique : Balisage

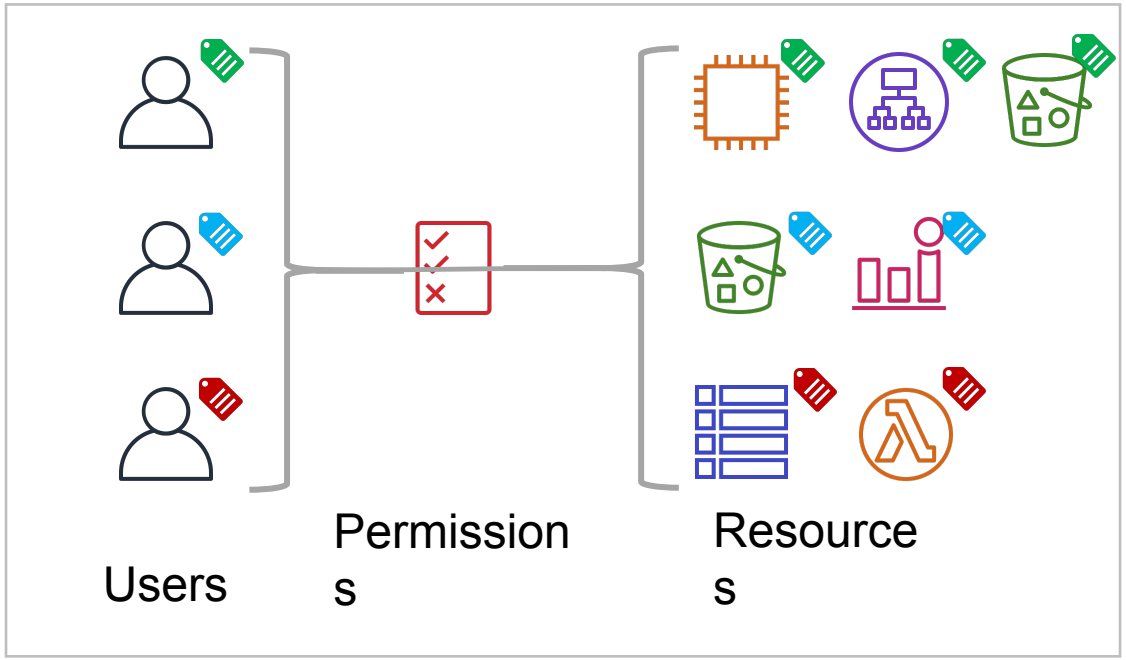
- Une balise se compose d'un nom et (éventuellement) d'une valeur.
  - Elle peut être appliquée à des ressources sur l'ensemble de vos comptes AWS.
  - Les clés et les valeurs des balises sont renvoyées par de nombreuses opérations API différentes.
- Définir des balises personnalisées
- Nombreuses utilisations pratiques
  - Facturation, vues filtrées, contrôle d'accès, etc.
- Exemple de balises appliquées à une instance EC2 :
  - Nom = serveur web
  - Projet = licorne
  - Pile = dev

Les étiquettes peuvent également être appliquées aux utilisateurs ou aux rôles IAM, par exemple -



Attribute-based access control (ABAC)

- Approche hautement évolutive du contrôle d'accès
  - Les attributs sont une clé ou une paire clé-valeur, telle qu'une balise.
  - **Exemple d'attributs**
    - Équipe = Développeurs
    - Projet = Licorne
- Les règles de permission (politique) sont plus faciles à maintenir avec ABAC qu'avec RBAC.
- **Avantages**
  - Les permissions s'appliquent automatiquement, sur la base des attributs
  - Des permissions granulaires sont possibles sans qu'il soit nécessaire de mettre à jour les permissions pour chaque nouvel utilisateur ou nouvelle ressource.
  - Entièrement auditable



Appliquer ABAC à votre organisation

Comment appliquer ABAC à votre organisation :

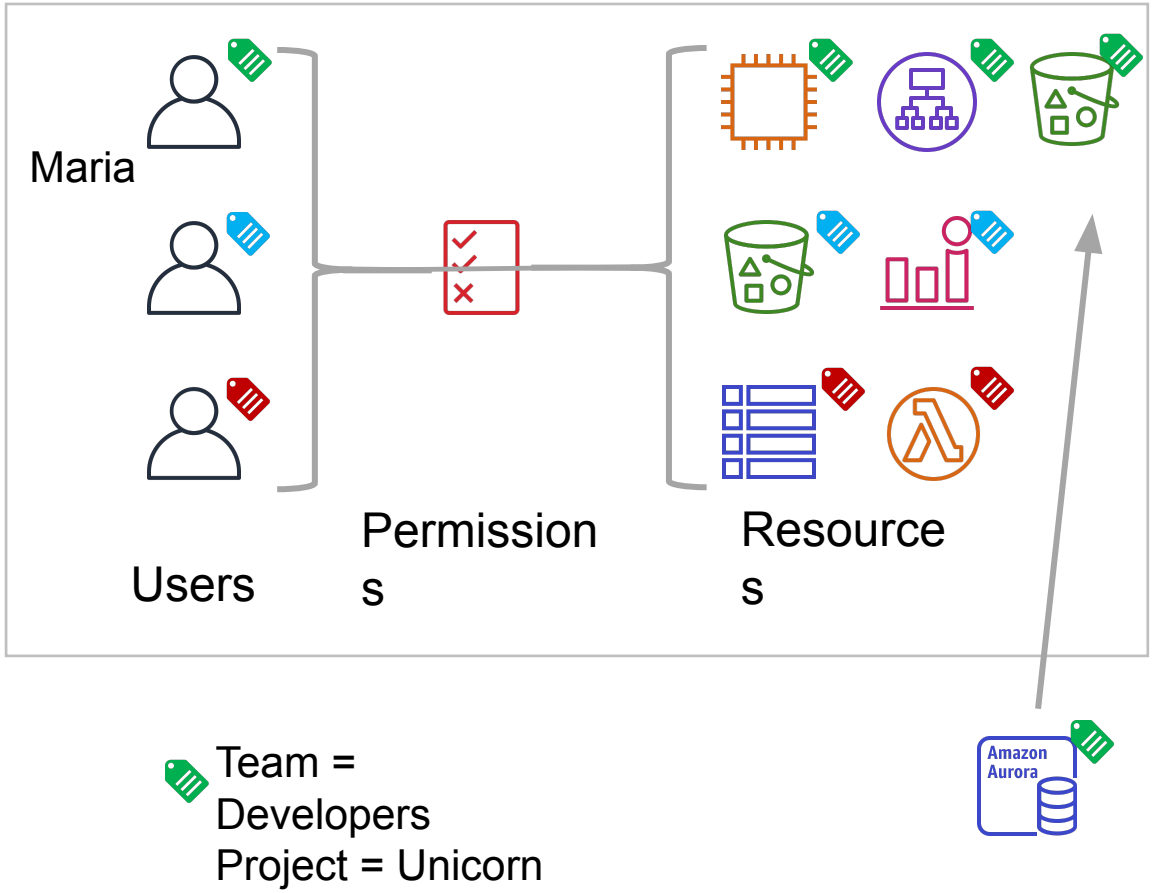
a) Définir des attributs de contrôle d'accès pour les identités

b) Exiger des attributs pour les nouvelles ressources

c) Configurer les autorisations en fonction des attributs

d) Test

- Créer de nouvelles ressources
- Vérifier que les autorisations s'appliquent automatiquement



Utilisateurs authentifiés en externe

- Fédération d'identité
- Authentification de l'utilisateur par un système externe au compte AWS.
    - Exemple : annuaire d'entreprise
- Elle permet d'autoriser l'accès par le biais d'identités existantes, sans créer d'utilisateurs IAM.

Options de fédération d'identité

1. AWS STS
    - Fournisseurs de services d'identité publics (IdP)
    - Application personnalisée de courtier en identité
2. Langage de marquage d'assertion de sécurité (SAML)
3. Amazon Cognito

Vue d'ensemble d'authentification IdP

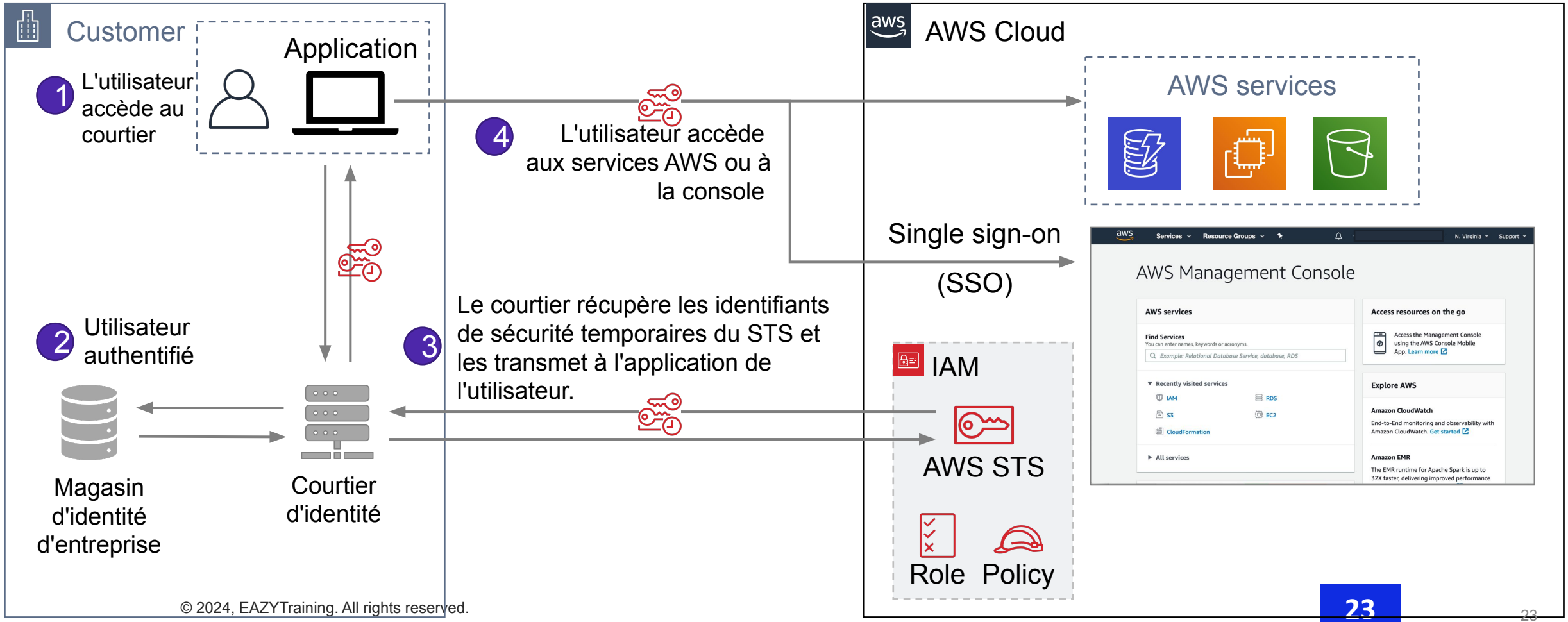
User accesses identity broker via application

Identity broker authenticates user

Requests temporary credentials from AWS STS

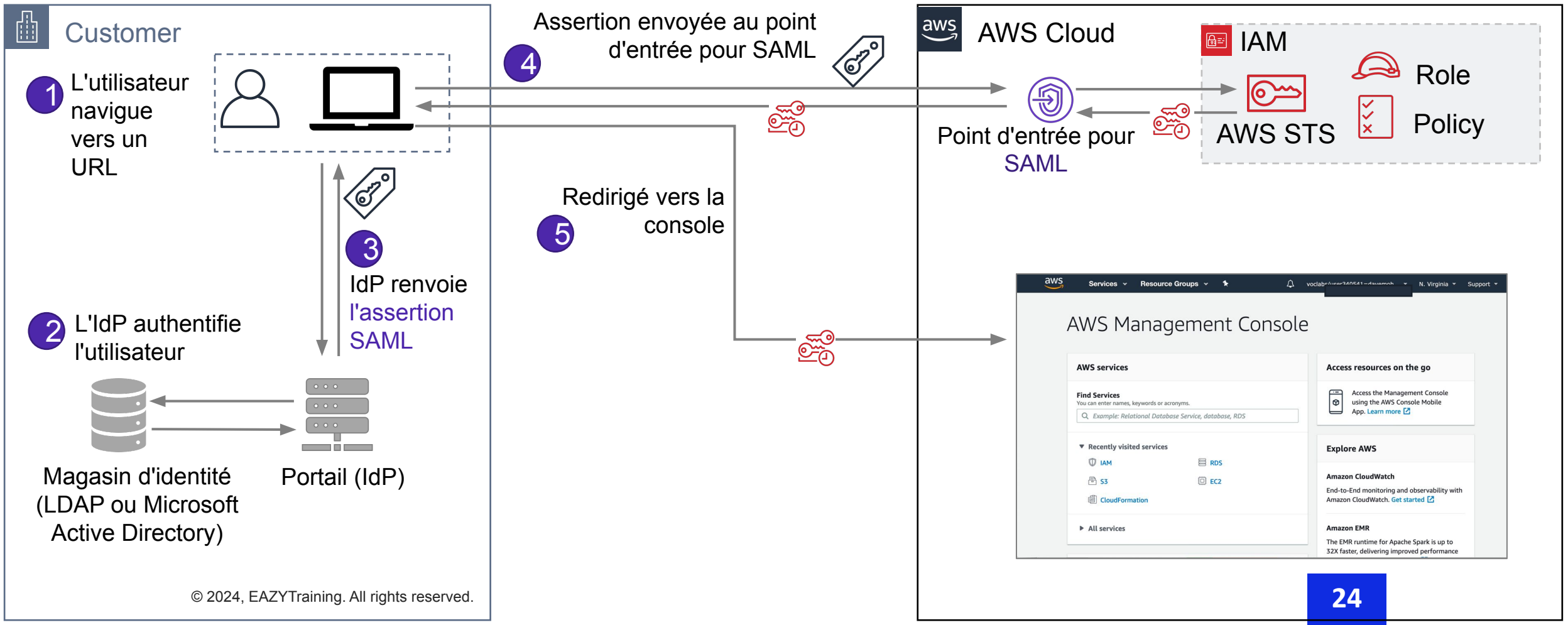
Temporary credentials returned to application

Fédération d'identité avec un courtier ou broker d'identité



23

Fédération d'identité à l'aide de SAML



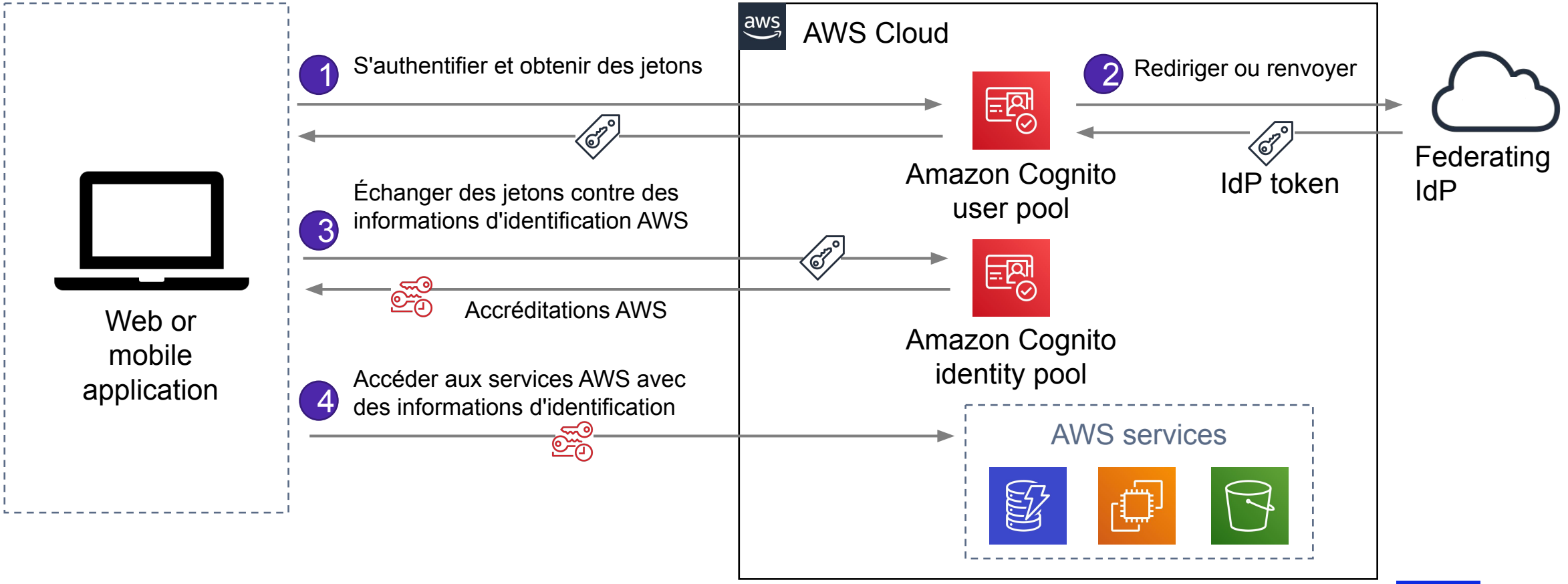
Amazon Cognito

Amazon Cognito

Amazon Cognito est un service entièrement géré.

- Il fournit l'authentification, l'autorisation et la gestion des utilisateurs pour les applications web et mobiles.
- Amazon Cognito fournit une fédération d'identité web
  - Il peut être utilisé comme courtier d'identité qui prend en charge les IdP compatibles avec OpenID Connect (OIDC).
- **Identités fédérées**
  - Les utilisateurs se connectent avec des fournisseurs d'identité sociale (Amazon, Facebook, Google) ou avec SAML.
- **Pools d'utilisateurs**
  - Vous pouvez maintenir un répertoire avec des profils d'utilisateurs et des jetons d'authentification.

Exemple d'Amazon Cognito



Points clés

- Les rôles AM fournissent des identifiants de sécurité temporaires pouvant être assumés par une personne, une application ou un service.
- Le service de jetons de sécurité AWS (AWS STS) vous permet de demander des informations d'identification AWS temporaires.
- Avec la fédération d'identité, l'authentification de l'utilisateur est externe au compte AWS.
    - Réalisée à l'aide d'AWS STS, de SAML ou d'Amazon Cognito.

Lab

Création des utilisateurs IAM, création d'un groupe, ajout des utilisateurs dans le groupe et association des autorisations au groupe.

Résumé

En résumé, dans ce module, vous avez appris à :

- Expliquer l'objectif des utilisateurs, groupes et rôles de la gestion des identités et des accès (IAM) d'AWS
- Décrire comment permettre la fédération des utilisateurs au sein d'une architecture afin de renforcer la sécurité
- Configuration des utilisateurs IAM

MERCI POUR VOTRE AIMABLE ATTENTION!

EAZYTraining

Alphonsine Lahda

Lahda Biassou Alphonsine

Ingénieure cloud et Formatrice