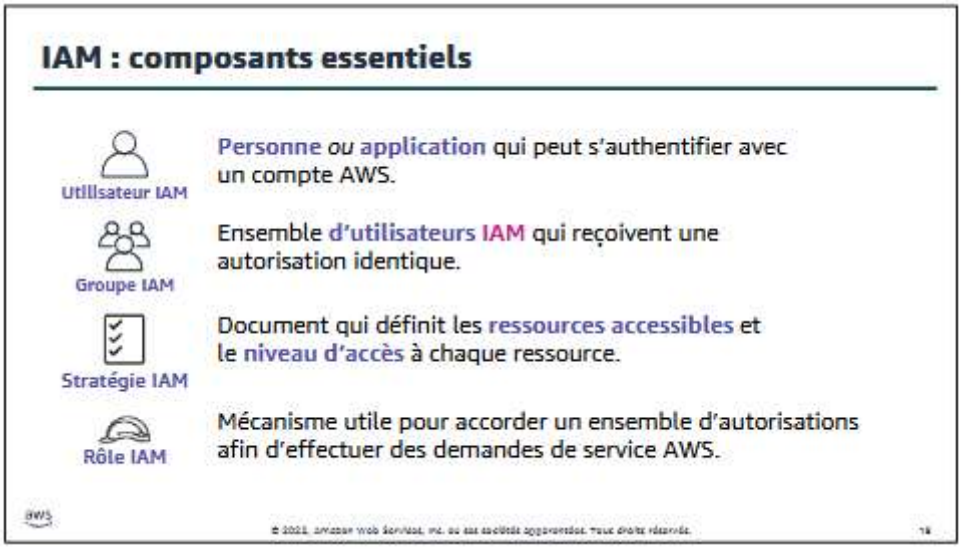
AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) permet de contrôler les accès aux services de calcul, de stockage, de base de données et d'application dans AWS Cloud. IAM peut être utilisé pour gérer l'authentification et pour spécifier et appliquer des stratégies d'autorisation pour vous permettre de spécifier quels utilisateurs peuvent accéder à quels services.

IAM est un outil qui gère de manière centralisée l'accès aux ressources de lancement, de configuration, de gestion et de résiliation de votre compte AWS. Il implique un contrôle précis de l'accès aux ressources, y compris la possibilité de spécifier exactement quels appels d'API l'utilisateur est autorisé à effectuer pour chaque service.

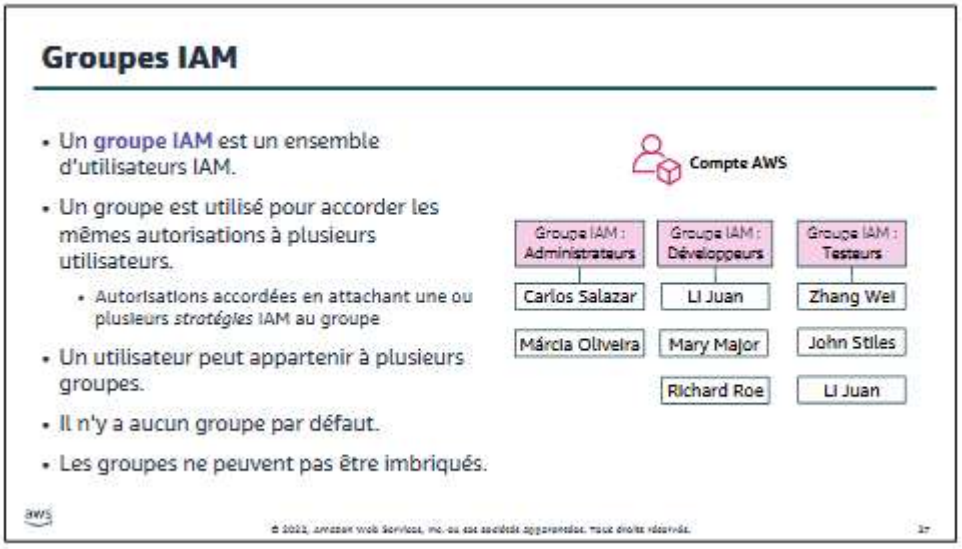
Avec IAM, il est possible de gérer quelles ressources sont accessibles à quels utilisateurs et comment ils peuvent y accéder. Par exemple, on peut accorder à certains utilisateurs un accès complet à Amazon EC2, Amazon S3, Amazon DynamoDB, Amazon Redshift et d'autres services AWS.

Cependant, pour d'autres utilisateurs, vous pouvez autoriser uniquement l'accès en lecture seule à quelques compartiments S3. De même, vous pouvez autoriser d'autres utilisateurs à administrer uniquement des instances EC2 spécifiques. Vous pouvez également autoriser quelques utilisateurs à accéder uniquement aux informations de facturation du compte et à rien d'autre.

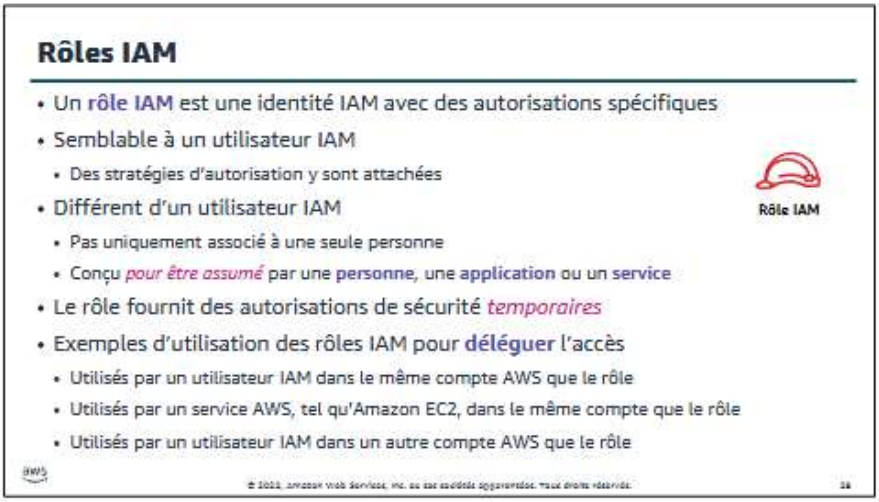


Un utilisateur IAM est une personne ou une application qui est définie dans un compte AWS et qui doit effectuer des appels d'API vers les produits AWS. Chaque utilisateur doit posséder un nom unique (sans espaces dans le nom) dans le compte AWS et un ensemble d'autorisations de sécurité qui ne sont pas partagées avec d'autres utilisateurs. Ces autorisations sont différentes des autorisations de sécurité de l'utilisateur racine du compte AWS. Chaque utilisateur est défini dans un seul compte AWS.

Un groupe IAM est un ensemble d'utilisateurs IAM. Les groupes IAM simplifient la spécification et la gestion des autorisations pour plusieurs utilisateurs.

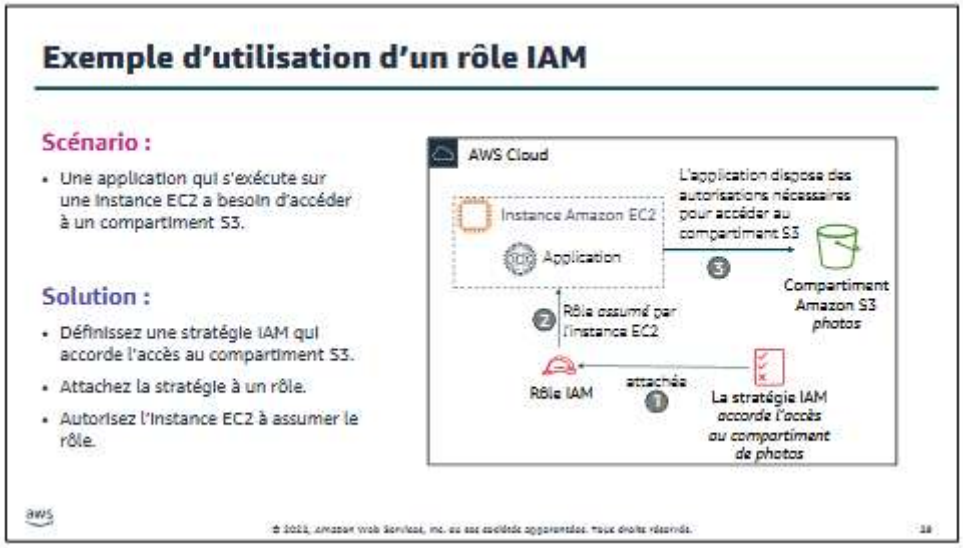


Un rôle IAM est un outil permettant d'accorder un accès temporaire à des ressources AWS spécifiques dans un compte AWS.



Similaire à un utilisateur IAM, car il s'agit également d'une identité AWS à laquelle il est possible d'attacher des stratégies d'autorisation, et ces autorisations déterminent ce que l'identité peut et ne peut pas faire dans AWS.

Cependant, au lieu d'être associé à **une seule personne**, un rôle peut être endossé par **tous ceux qui en ont besoin**. En outre, un rôle ne dispose pas d'informations d'identification standard à long-terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des autorisations de sécurité temporaires pour votre session de rôle.



Dans ce diagramme, un développeur exécute une application sur une instance EC2 qui nécessite l'accès au compartiment S3 qui est nommé photos. Un administrateur crée le rôle IAM et l'attache à l'instance EC2. Ce rôle inclut une stratégie d'autorisations qui accorde un accès en lecture seule au compartiment S3 spécifié. Il comprend également une stratégie de confiance qui permet à l'instance EC2 d'endosser le rôle et de récupérer les autorisations temporaires. Lorsque l'application s'exécute sur l'instance, elle peut accéder au compartiment photos avec les autorisations temporaires du rôle. L'administrateur n'a pas besoin d'accorder au développeur l'autorisation d'accéder au compartiment photos, et le développeur n'a à aucun moment besoin de partager ni de gérer ses autorisations.

Un rôle IAM ne donne pas d'autorisations par lui-même ; ce sont les stratégies IAM attachées au rôle qui les accordent.

Une stratégie IAM est un document qui définit les autorisations permettant de déterminer les opérations que les utilisateurs peuvent effectuer dans le compte AWS. Une stratégie accorde généralement l'accès à des ressources spécifiques et définit les actions que l'utilisateur peut effectuer avec ces ressources. Les stratégies peuvent également refuser explicitement l'accès.

Par exemple, vous pouvez associer une stratégie à des ressources AWS de manière à bloquer toutes les requêtes ne provenant pas d'une plage d'adresses IP approuvées. Les stratégies spécifient les actions qui sont autorisées, sur quelles ressources autoriser les actions et l'effet que cela aura lorsque l'utilisateur sollicitera l'accès aux ressources.

L'ordre d'évaluation des stratégies n'a aucun impact sur le résultat de l'évaluation. Toutes les stratégies sont évaluées et le résultat indique toujours si la demande est autorisée ou refusée. En cas de conflit, la stratégie la plus restrictive prime.

Lorsqu'un utilisateur IAM est créé, il faudra sélectionner le type d'accès qui lui est attribué pour accéder aux ressources AWS.

Il existe deux types d'accès différents aux utilisateurs:

- L'accès par programmation
- L'accès à AWS Management Console.

Un **accès par programmation**, l'utilisateur IAM devra présenter un ID de clé d'accès et une clé d'accès secrète lorsqu'il effectuera un appel d'API AWS à l'aide de l'AWS CLI, du kit SDK AWS ou d'un autre outil de développement.

L'accès à **AWS Management Console**, l'utilisateur IAM devra fournir l'ID de compte à 12 chiffres ou l'alias de compte correspondant mais également son nom d'utilisateur et son mot de passe IAM.

Pour attribuer une autorisation à un utilisateur, un groupe ou un rôle, il faut une stratégie IAM (ou rechercher une stratégie existante dans le compte).

Cette stratégie IAM est une déclaration formelle des autorisations qui sont accordées à une entité. Les stratégies peuvent être attachées à n'importe quelle entité IAM. Parmi les entités, citons les utilisateurs, les groupes, les rôles ou les ressources.

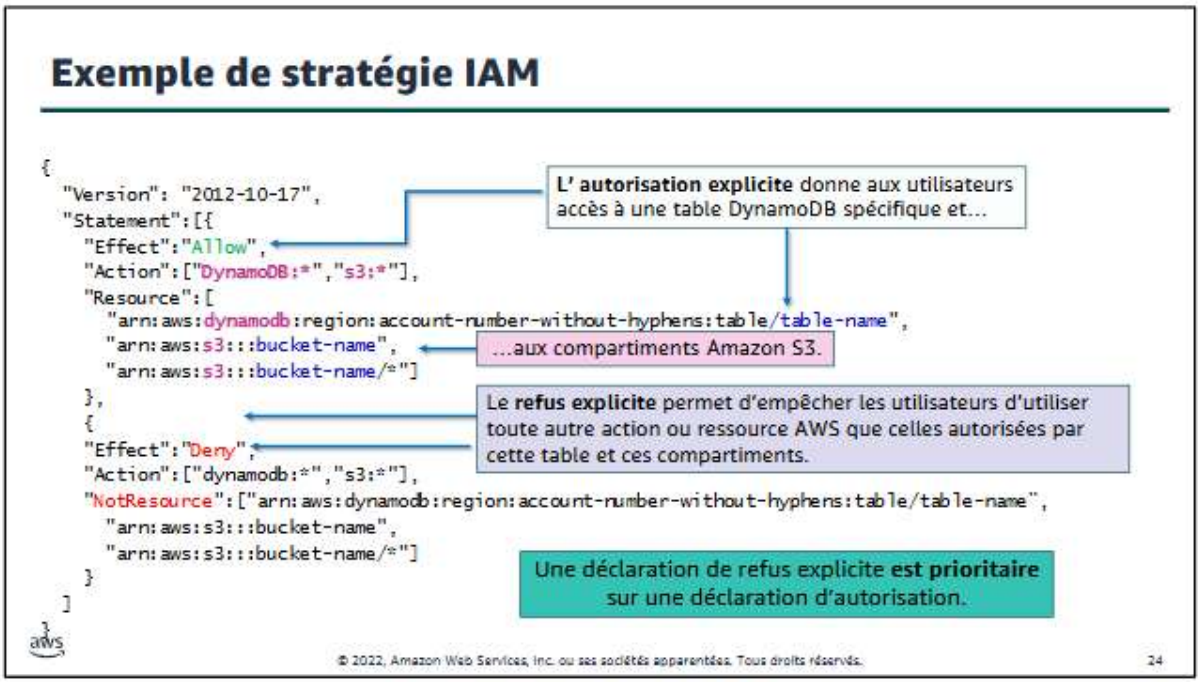
Par exemple, il est possible d'associer une stratégie à des ressources AWS de manière à bloquer toutes les requêtes ne provenant pas d'une plage d'adresses IP approuvées. Les stratégies spécifient les actions qui sont autorisées, sur quelles ressources autoriser les actions et l'effet que cela aura lorsque l'utilisateur sollicitera l'accès aux ressources.

Il existe deux types de stratégies IAM. Les stratégies basées sur l'identité sont des stratégies attachées à un mandataire ou à une identité, comme un utilisateur, un rôle ou un groupe IAM. Ces stratégies contrôlent les actions que peut effectuer cette identité, sur quelles ressources et dans quelles conditions. Les stratégies basées sur l'identité peuvent être classées comme suit:

Stratégies gérées: stratégies autonomes basées sur une identité que vous pouvez attacher à plusieurs utilisateurs, groupes et rôles dans votre compte AWS.

Stratégies intégrées: stratégies que vous créez et gérez et qui sont intégrées directement à un utilisateur, groupe ou rôle.

Les stratégies basées sur les ressources sont des documents de stratégie au format JSON associez à une ressource, telle qu'un compartiment S3. Ces stratégies contrôlent les actions qu'un mandataire spécifique peut effectuer sur cette ressource et dans quelles conditions.



Il n'existe aucune autorisation par défaut. Toutes les actions du compte sont refusées à l'utilisateur par défaut (refus implicite) à moins que ces actions ne soient explicitement autorisées. Toute action que vous n'autorisez pas explicitement est refusée. Toute action que vous refusez de façon explicite sera toujours refusée.