AWS IAM Identity Center

AWS IAM Identity Center (successeur de AWS Single Sign-On) permet à plusieurs utilisateurs d'un Compte AWS unique d'utiliser les services d'AWS.

Utilisateur racine (root) d'un compte AWS

Présentation

- Lien : https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_root-user.html

Lors de la création d'un compte Amazon Web Services (AWS), cette identité de connexion dispose d'un accès complet à tous les services et ressources AWS du compte.

Cette identité est appelée l'**utilisateur racine (root)** du compte AWS et la connexion à ce compte utilise l'adresse e-mail et le mot de passe qui a été utilisés à la création du compte.

> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour ses tâches quotidiennes, y compris pour les tâches administratives. Les informations d'identification de l'utilisateur root ne servent qu'à effectuer certaines tâches de gestion des comptes et des services.
>
> - Lien : https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/best-practices.html
> - Tâche qui nécessitent d'être utilisateur racine : https://docs.aws.amazon.com/fr_fr/accounts/latest/reference/root-user-tasks.html

Clé d'accès

Il est possible de créer une clé d'accès utile pour les appels de CLI et d'API. Il n'sty possible de créer que deux clés d'accès pour chaque utilisateur, racine ou IAM.

> Un **clé d'accès** est un ensemble constitué d'un **ID de clé** d'accès et d'une **clé d'accès secrète**.

Authentification multifactorielle (MFA)

Il est conseillé d'ctiver l'authentification multifactorielle (MFA) pour l'utilisateur root.

- Lien : https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-root

Utilisateur administratif

Création d'un utilisateur administratif

A la suite de la création du compte AWS (utilisateur récine), il est conseillé de créer un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

- Lien : https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/getting-started.html

Étape 1 : activer IAM Identity Center

Étape 2 : choix de votre source d'identité

Étape 3 : création d'un jeu d'autorisations administratives

Il est nécessaire de créer un jeu d'autorisations **AdministratorAccess** dans la section **Type de jeu d'autorisations** en choisissant

Ensemble d'autorisations prédéfini.

Les paramètres par défaut accordent un accès complet aux AWS services et aux ressources à l'aide de cet ensemble d'autorisations AdministratorAccess prédéfini.

Le paramètre par défaut limite la session à une heure.

- Lien : https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/get-started-create-an-administrative-permission-set.html

Étape 4 : configurer Compte AWS l'accès pour un utilisateur administratif

- Ouvrir la console IAM Identity Center : https://console.aws.amazon.com/singlesignon
- Dans le volet de navigation, sous **Autorisations multi-comptes**, choisir **Comptes AWS**.
- Sur la page **Comptes AWS**, dans la liste arborescente de l'organisation, sélectionnerz la case à cocher pour le compte Compte AWS qui est **compte de gestion** et pour lequel vous souhaitez attribuer un accès administratif.
- Cliquer sur le bouton **Attribuer des utilisateurs ou des groupes**.
    - Etape 1 : sélectionner ou créer au préalable l'utilisateur / groupe à qui les autorisations administratives seront attribuées.
    - Etape 2 : Sélectionner comme ensemble d'autorisations **AdministratorAccess**ensemble d'autorisations. Si nécessaire, créer un ensemble d'autorisations de type **Jeu d'autorisations prédéfini** avec la politique **AdministratorAccess**
    - Etape 3 : valider
- Lien : https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/get-started-assign-account-access-admin-user.html

Activer le MFA pour IAM Identity Center :

- https://docs.aws.amazon.com/fr_fr/singlesignon/latest/userguide/mfa-enable-how-to.html

Étape 5 : Connectez-vous au portail d'AWSaccès à l'aide de vos informations d'identification administratives

IAM Identity Center permet d'attribuer plusieurs ensembles d'autorisations au même utilisateur. Afin de suivre les meilleures pratiques consistant à appliquer les autorisations de moindre privilège et après avoir créé l'utilisateur administratif, créez un ensemble d'autorisations plus restrictif et attribuez-le au même utilisateur.

De cette manière, vous pouvez accéder à votre compte uniquement Compte AWS avec les autorisations dont vous avez besoin, plutôt qu'avec des autorisations administratives.

Pour avoir un profil **développeur** pour le même compte utilisateur administratif dans IAM Identity Center :

- créer un nouvel ensemble d'autorisations **PowerUserAccess des autorisations** qui ne permet pas la gestion des utilisateurs et des groupes
- attribuer ce jeu d'autorisations au même utilisateur.
- Lors de la connexion au portail AWS d'accès pour accéder à votre AWS compte, il est alors possible de choisir d'effectuer des tâches de développement dans le compte PowerUserAccess plutôt que de le AdministratorAccess.

Étape 6 : Création d'un ensemble d'autorisations qui applique les autorisations de moindre privilège

Étape 7 : Configuration de Compte AWS l'accès pour des utilisateurs supplémentaires (facultatif)

Étape 8 : Configuration de l'accès par authentification unique à vos applications (facultatif)

Connexion en tant qu'utilisateur administratif

Pour se connecter avec l'utilisateur administratif IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.