Atelier 1 : Introduction à AWS IAM

La **Gestion des identités et des accès AWS (AWS IAM)** est un service web qui permet aux clients d'Amazon Web Services (AWS) de gérer leurs utilisateurs et les autorisations qui leur sont associées dans AWS. Avec IAM, vous pouvez gérer de façon centralisée les **utilisateurs**, les **identifiants de sécurité** tels que les clés d'accès, et les **autorisations** qui déterminent les ressources AWS auxquelles les utilisateurs peuvent accéder.

Présentation de l'atelier et des objectifs

Cet atelier explique les opérations suivantes :

- Exploration des **utilisateurs et groupes IAM** pré-créés
- Inspection des **politiques IAM** appliquées aux groupes pré-créés

- Suivi d'un **scénario réel** en ajoutant des utilisateurs à des groupes et en activant des capacités spécifiques
- Localisation et utilisation de l'**URL de connexion IAM**
- **Test** des effets des politiques sur l'accès aux services

Restrictions des services AWS

Dans l'environnement de cet atelier, les services AWS et actions de service auxquels vous avez accès pourraient être limités à ceux dont vous avez besoin pour exécuter les instructions de l'atelier. Des erreurs peuvent survenir si vous tentez d'accéder à d'autres services ou d'effectuer des actions au-delà de celles décrites dans cet atelier.

Gestion des identités et des accès AWS

La Gestion des identités et des accès AWS (AWS IAM) peut être utilisée pour les opérations suivantes :

- **Gestion des utilisateurs IAM et de leur accès :** vous pouvez créer des utilisateurs et leur assigner des identifiants de sécurité individuels (clés d'accès, mots de passe et dispositifs d'authentification multi-facteurs). Vous pouvez gérer les autorisations pour contrôler les opérations qu'un utilisateur peut effectuer.
- **Gestion des rôles IAM et de leurs autorisations :** un rôle IAM est semblable à un utilisateur, dans le sens où il s'agit d'une identité AWS dotée de politiques d'autorisations qui 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.
- **Gestion des utilisateurs fédérés et de leurs autorisations :** vous pouvez activer la *fédération d'identité* pour autoriser les utilisateurs existants de votre entreprise à accéder à la Console de gestion AWS, à appeler des API AWS et à accéder à des ressources, sans avoir à créer un utilisateur IAM pour chaque identité.

Durée

Cet atelier dure environ **40 minutes**.

Accès à la Console de gestion AWS

1. En haut à droite de ces instructions, choisissez **Start Lab** (Démarrer l'atelier).
    - La session commence.
    - Un minuteur s'affiche en haut de la page et indique le temps restant dans la session.

Conseil : pour actualiser la durée de la session, vous pouvez à tout moment sélectionner à nouveau **Start Lab** (Démarrer l'atelier) avant que le minuteur n'atteigne 0:00.

- Avant de continuer, attendez que l'icône circulaire située à droite du lien AWS dans le coin supérieur gauche devienne verte.

2. Pour vous connecter à la Console de gestion AWS, choisissez le lien **AWS** dans le coin supérieur gauche.
    - Un nouvel onglet de navigateur s'ouvre et vous connecte à la console.

Conseil : si aucun nouvel onglet ne s'ouvre, une bannière ou une icône, généralement située en haut du navigateur, indique que celui-ci empêche le site d'ouvrir des fenêtres contextuelles. Cliquez sur la bannière ou l'icône, puis sélectionnez **Allow pop-ups** (Autoriser les fenêtres contextuelles).

3. Disposez l'onglet Console de gestion AWS de façon à l'afficher à côté de ces instructions. Dans l'idéal, vous devez pouvoir visualiser les deux onglets en même temps pour suivre plus facilement les étapes de l'atelier.

Obtention de crédit pour votre travail

À la fin de cet atelier, vous apprendrez à envoyer l'atelier afin de recevoir un score basé sur votre progression.

Conseil : le script qui vérifie votre travail peut ne vous attribuer des points que si vous nommez les ressources et définissez les configurations comme indiqué. En particulier, les valeurs dans ces instructions qui apparaissent dans This Format doivent être saisies exactement telles que documentées (sensibles à la casse).

Tâche 1 : Exploration des utilisateurs et des groupes

Dans cette tâche, vous allez explorer les groupes et les utilisateurs qui ont déjà été créés pour vous dans IAM.

4. Dans la zone de recherche, à droite de **Services**, recherchez et choisissez **IAM** pour ouvrir la console IAM.
5. Dans le volet de navigation de gauche, choisissez **Utilisateurs**.

Les utilisateurs IAM suivants ont été créés pour vous :

- user-1
- user-2
- user-3

6. Choisissez le lien **user-1**.

Cela vous dirige vers la page récapitulative de l'utilisateur user-1. L'onglet **Autorisations** s'affiche.

7. Remarquez que l'utilisateur user-1 ne dispose d'aucune autorisation.
8. Choisissez l'onglet **Groupes**.

L'utilisateur user-1 n'est membre d'aucun groupe.

9. Choisissez l'onglet **Informations d'identification de sécurité**.

Un **mot de passe de console** est attribué à l'utilisateur user-1.

10. Dans le volet de navigation de gauche, choisissez **Groupes d'utilisateurs**.

Les groupes suivants ont déjà été créés pour vous :

- EC2-Admin
- EC2-Support
- S3-Support

11. Sélectionnez le lien du groupe **EC2-Support**.

Cela vous dirige vers la page récapitulative du groupe **EC2-Support**.

12. Choisissez l'onglet **Autorisations**.

Une politique gérée appelée **AmazonEC2ReadOnlyAccess** est associée à ce groupe. Les politiques gérées sont des politiques préconçues (par AWS ou par vos administrateurs) qui peuvent être associées aux utilisateurs et aux groupes IAM. Lorsque la politique est mise à jour, les changements s'appliquent immédiatement à tous les utilisateurs et groupes qui sont associés à cette politique.

13. Choisissez l'icône plus (**+**) en regard de la politique AmazonEC2ReadOnlyAccess pour en afficher les détails.

Remarque : une politique définit les actions autorisées ou refusées pour des ressources AWS spécifiques.

Cette politique accorde l'autorisation de répertorier et de décrire les informations à propos d'EC2, d'Elastic Load Balancing, de CloudWatch et d'Auto Scaling. La capacité de voir ses ressources sans les modifier est idéale pour un rôle de support.

La structure de base des déclarations d'une politique IAM est la suivante :

- **Effet** propose l'option *Autoriser* ou *Refuser* pour autoriser ou refuser les autorisations.
- **Action** indique les appels d'API qui peuvent être effectués auprès d'un service AWS (par exemple, *cloudwatch:ListMetrics*).

- **Ressource** définit la portée des entités concernées par la règle de la politique (par exemple, un compartiment Amazon S3 ou une instance Amazon EC2 spécifique, ou * qui signifie *n'importe quelle ressource*).

14. Choisissez l'icône moins (**-**) pour masquer les détails de la politique.

15. Dans le volet de navigation de gauche, choisissez **Groupes d'utilisateurs**.

16. Choisissez le lien du groupe **S3-Support**, puis choisissez l'onglet **Autorisations**.

Le groupe S3-Support est associé à la politique **AmazonS3ReadOnlyAccess**.

17. Choisissez l'icône plus (**+**) pour afficher les détails de la politique.

Cette politique accorde les autorisations Get et List permettant d'obtenir et de répertorier les ressources dans Amazon S3.

18. Choisissez l'icône moins (**-**) pour masquer les détails de la politique.

19. Dans le volet de navigation de gauche, choisissez **Groupes d'utilisateurs**.

20. Choisissez le lien du groupe **EC2-Admin**, puis choisissez l'onglet **Autorisations**.

Ce groupe est légèrement différent des deux autres. Au lieu d'être associé à une *politique gérée*, il utilise une **politique en ligne**, laquelle est affectée à un seul utilisateur ou groupe. Les politiques intégrées sont généralement utilisées pour appliquer des autorisations à des situations exceptionnelles.

21. Choisissez l'icône plus (**+**) pour afficher les détails de la politique.

Cette politique accorde l'autorisation d'afficher (Describe) les informations à propos d'Amazon EC2. Elle offre également la possibilité de lancer et d'arrêter les instances.

22. Choisissez l'icône moins (**-**) pour masquer les détails de la politique.

Scénario métier

Pendant le reste de cet atelier, vous allez travailler avec ces utilisateurs et ces groupes pour activer les autorisations soutenant le scénario métier suivant :

Votre entreprise a de plus en plus recours à Amazon Web Services et utilise de nombreuses instances Amazon EC2 ainsi qu'une grande capacité de stockage Amazon S3. Vous souhaitez accorder l'accès à de nouveaux membres du personnel en fonction de leurs fonctions professionnelles :

Utilisateur	Dans le groupe	Autorisations
user-1	S3-Support	Read-Only access to Amazon S3 (Accès en lecture seule à Amazon S3)
user-2	EC2-Support	Read-Only access to Amazon EC2 (Accès en lecture seule à Amazon EC2)
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances (Afficher, démarrer et arrêter les insta Amazon EC2)

|

Tâche 2 : Ajout d'utilisateurs aux groupes

Vous avez récemment attribué à **user-1** un rôle qui lui permet de fournir du support pour Amazon S3. Vous allez l'ajouter au groupe **S3-Support** afin qu'il hérite des autorisations nécessaires grâce à la politique *AmazonS3ReadOnlyAccess* qui y est associée.

Vous pouvez ignorer toutes les erreurs « non autorisé » qui apparaissent durant cette tâche. Elles sont causées par les autorisations limitées de votre compte pour l'atelier. Cependant, elles ne vous empêcheront pas d'effectuer cet atelier.

Ajout de l'utilisateur user-1 au groupe S3-Support

23. Dans le volet de navigation gauche, choisissez **Groupes d'utilisateurs**.

24. Sélectionnez le lien du groupe **S3-Support**.

25. Choisissez l'onglet **Utilisateurs**.

26. Dans l'onglet **Utilisateurs**, choisissez **Ajouter des utilisateurs**.

27. Dans la fenêtre **Add Users to S3-Support** (Ajouter des utilisateurs au groupe S3-Support), configurez les éléments suivants :
    - Sélectionnez **user-1**.
    - En bas de l'écran, choisissez **Ajouter des utilisateurs**.

Dans l'onglet **Utilisateurs**, vous verrez que l'utilisateur user-1 a été ajouté au groupe.

Ajout de l'utilisateur user-2 au groupe EC2-Support

Vous avez attribué à **user-2** un rôle qui lui permet de fournir du support pour Amazon EC2.

28. En répétant les mêmes étapes que ci-dessus, ajoutez **user-2** au groupe **EC2-Support**.

L'utilisateur user-2 devrait désormais faire partie du groupe **EC2-Support**.

Ajout de l'utilisateur user-3 au groupe EC2-Admin

Vous avez attribué à **user-3** le rôle d'administrateur Amazon EC2, pour qu'il gère vos instances EC2.

29. En répétant les mêmes étapes que ci-dessus, ajoutez **user-3** au groupe **EC2-Admin**.

L'utilisateur user-3 devrait désormais faire partie du groupe **EC2-Admin**.

30. Dans le volet de navigation de gauche, choisissez **Groupes d'utilisateurs**.

Chaque groupe doit désormais avoir le chiffre **1** dans la colonne Utilisateurs, indiquant le nombre d'utilisateurs du groupe.

Si la valeur **1** n'apparaît pas en face de chaque groupe, revenez aux instructions précédentes pour vérifier que chaque utilisateur est affecté à un groupe d'utilisateurs, comme indiqué dans le tableau de la section Scénario métier.

Tâche 3 : Connexion et test des utilisateurs

Dans cette tâche, vous allez tester les autorisations de chaque utilisateur IAM.

31. Dans le volet de navigation de gauche, choisissez **Tableau de bord**.

Un lien **URL de connexion pour les utilisateurs IAM de ce compte** s'affiche à droite. Il est de la forme : *https://123456789012.signin.aws.amazon.com/console*

Ce lien peut être utilisé pour se connecter au compte AWS que vous utilisez actuellement.

32. Copiez l'**URL de connexion pour les utilisateurs IAM de ce compte** dans un éditeur de texte.

33. Ouvrez une fenêtre de navigation privée (Incognito).

Mozilla Firefox

- Choisissez les barres de menu en haut à droite de l'écran.
- Sélectionnez **New private window** (Nouvelle fenêtre privée).

Google Chrome

- Choisissez les points de suspension en haut à droite de l'écran.
- Sélectionnez **New Incognito Window** (Nouvelle fenêtre de navigation privée).

Microsoft Edge

- Choisissez les points de suspension en haut à droite de l'écran.
- Choisissez **New InPrivate window** (Nouvelle fenêtre InPrivate).

Microsoft Internet Explorer

- Choisissez l'option de menu **Outils**.
- Choisissez **InPrivate Browsing** (Navigation InPrivate).

34. Collez le lien de **connexion des utilisateurs IAM** dans la barre d'adresse de votre session privée de navigateur et appuyez sur **Entrée**.

Vous allez vous connecter en tant que **user-1**, qui s'est vu assigner un rôle au sein de votre équipe de support pour le stockage Amazon S3.

35. Connectez-vous à l'aide des informations suivantes :
    - **Nom utilisateur IAM :** user-1
    - **Mot de passe :** Lab-Password1

36. Dans le champ de recherche à droite de **Services**, recherchez et choisissez **S3** pour ouvrir la console S3.

37. Choisissez le nom du compartiment qui existe dans le compte et parcourez son contenu.

Votre utilisateur faisant partie du groupe **S3-Support** dans IAM, il a l'autorisation d'afficher la liste des compartiments Amazon S3 et leur contenu.

Remarque : le compartiment ne contient aucun objet.

À présent, vérifiez s'il a accès à Amazon EC2.

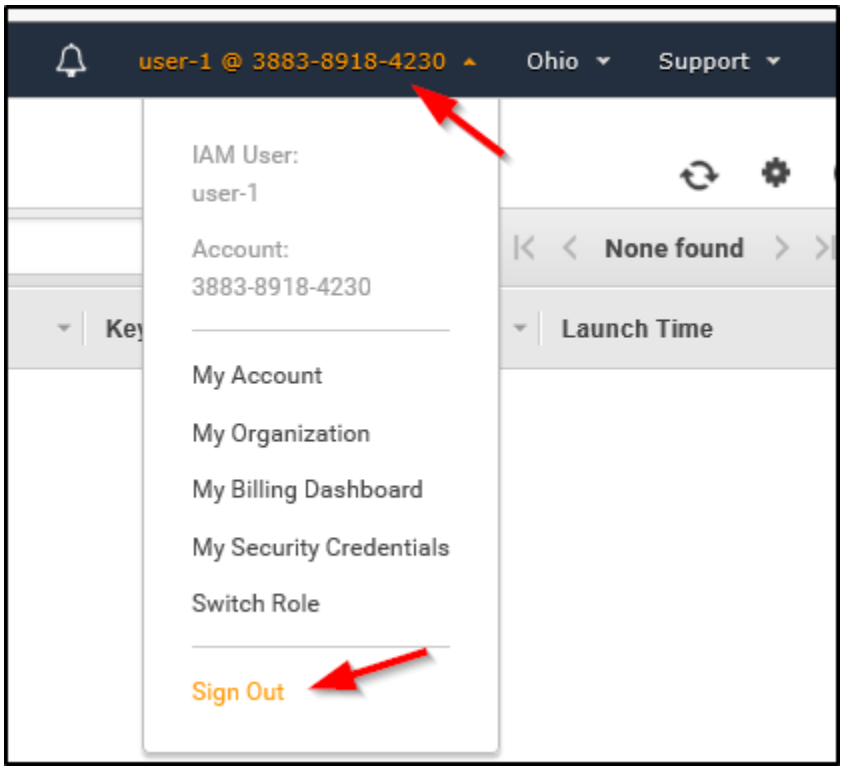
38. Dans la zone de recherche, à droite de **Services**, recherchez et choisissez **EC2** pour ouvrir la console EC2.

39. Dans le volet de navigation gauche, choisissez **Instances**.

Aucune instance n'est visible. En revanche, vous voyez un message stipulant : *You are not authorized to perform this operation* (Vous n'êtes pas autorisé à effectuer cette opération). Vous recevez ce message, car aucune autorisation n'a été assignée à votre utilisateur pour accéder à Amazon EC2.

Vous allez vous connecter en tant que **user-2**, qui s'est vu assigner un rôle au sein de votre équipe de support Amazon EC2.

40. Déconnectez l'utilisateur user-1 de la **Console de gestion AWS** en effectuant les opérations suivantes :
    - En haut de l'écran, choisissez **user-1**.
    - Choisissez **Sign out** (Se déconnecter).



41. Collez le lien de **connexion des utilisateurs IAM** dans la barre d'adresse de l'onglet privé de votre navigateur et appuyez sur **Entrée**.

Remarque : ce lien devrait se trouver dans votre éditeur de texte.

42. Connectez-vous à l'aide des informations suivantes :
    - **Nom utilisateur IAM :** user-2
    - **Mot de passe :** Lab-Password2

43. Dans la zone de recherche, à droite de **Services**, recherchez et choisissez **EC2** pour ouvrir la console EC2.

44. Dans le volet de navigation de gauche, choisissez **Instances**.

Vous pouvez désormais voir une instance Amazon EC2, car vous bénéficiez d'autorisations de lecture seule. Cependant, vous ne pouvez apporter aucune modification aux ressources Amazon EC2.

Si vous ne voyez aucune instance Amazon EC2, votre région est peut-être incorrecte. En haut à droite de l'écran, déroulez le menu Région et sélectionnez la région que vous avez notée au début de l'atelier (par exemple, **Virginie du Nord**).

- Sélectionnez l'instance nommée *LabHost*.

45. Dans le menu **État de l'instance**, sélectionnez **Arrêter l'instance**.

46. Dans la fenêtre **Arrêter l'instance**, sélectionnez **Arrêter**.

Vous recevrez l'erreur suivante : *You are not authorized to perform this operation* (Vous n'êtes pas autorisé à effectuer cette opération). Vous voyez ainsi que cette politique vous permet uniquement d'afficher les informations, sans pouvoir les modifier.

47. Choisissez le signe X pour fermer le message *Failed to stop the instance* (Échec de l'arrêt de l'instance).

Vérifiez ensuite si l'utilisateur user-2 peut accéder à Amazon S3.

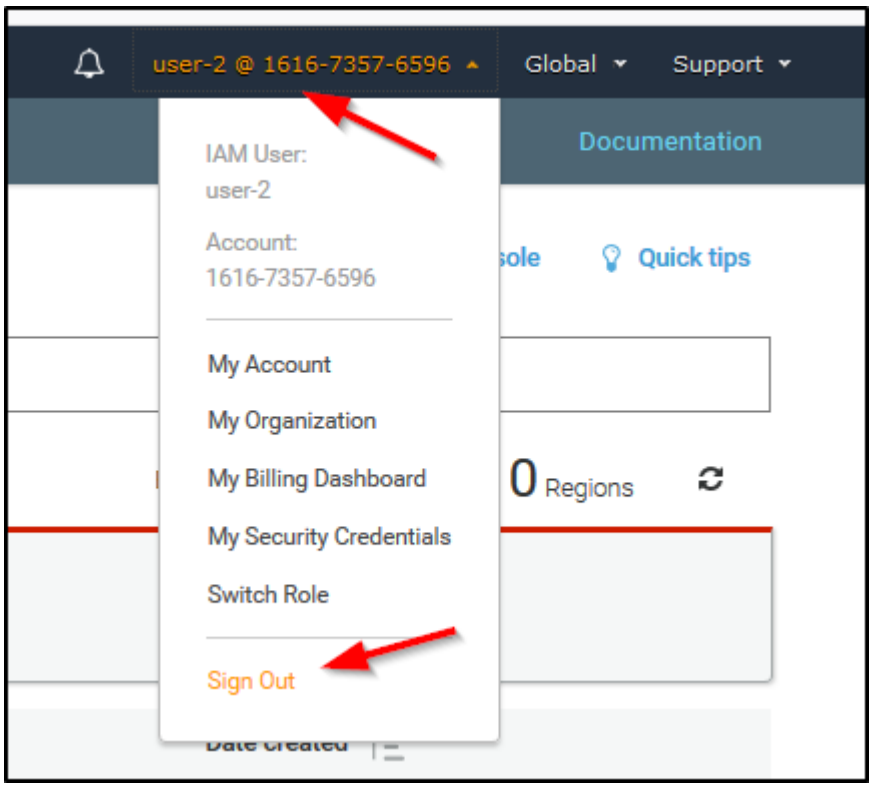
48. Dans le champ de recherche à droite de **Services**, recherchez et choisissez **S3** pour ouvrir la console S3.

Le message d'erreur **You don't have permissions to list buckets** (Vous n'êtes pas autorisé à répertorier les compartiments) s'affiche, car l'utilisateur user-2 n'a pas l'autorisation nécessaire pour accéder à Amazon S3.

Vous allez vous connecter à présent en tant que **user-3**, qui s'est vu attribuer un rôle d'administrateur pour Amazon EC2.

49. Déconnectez l'utilisateur user-2 de la **Console de gestion AWS** en effectuant les opérations suivantes :

    - En haut de l'écran, choisissez **user-2**.
    - Choisissez **Sign out** (Se déconnecter).



50. Collez le lien de **connexion des utilisateurs IAM** dans votre fenêtre de navigation privée et appuyez sur **Entrée**.

51. Collez à nouveau le lien de connexion dans la barre d'adresse de l'onglet de navigation privée de votre navigateur web. S'il ne figure pas dans le presse-papier, récupérez-le dans l'éditeur de texte où vous l'avez stocké auparavant.

52. Connectez-vous à l'aide des informations suivantes :
    - **Nom utilisateur IAM :** user-3
    - **Mot de passe :** Lab-Password3

53. Dans la zone de recherche, à droite de **Services**, recherchez et choisissez **EC2** pour ouvrir la console EC2.

54. Dans le volet de navigation de gauche, choisissez **Instances**.

En tant qu'administrateur Amazon EC2, vous devez avoir maintenant l'autorisation d'arrêter l'instance Amazon EC2.

Sélectionnez l'instance nommée *LabHost*.

Si vous ne voyez aucune instance Amazon EC2, votre région est peut-être incorrecte. En haut à droite de l'écran, déroulez le menu Région et sélectionnez la région que vous avez notée au début de l'atelier (par exemple, **Virginie du Nord**).

55. Dans le menu **État de l'instance**, choisissez **Arrêter l'instance**.

56. Dans la fenêtre **Arrêter l'instance**, choisissez **Arrêter**.

L'état de l'instance devient *arrêt* et l'instance s'arrête.

57. Fermez votre fenêtre de navigation privée.

Envoi de votre travail

58. Pour enregistrer votre progression, sélectionnez **Envoyer** en haut de ces instructions.

Important : certaines vérifications faites par le processus de soumission dans cet atelier ne vous donneront du crédit que si 5 minutes minimum se sont écoulées depuis que vous avez réalisé cette action. Si vous ne recevez pas de crédit lors de votre premier envoi, attendez quelques minutes et effectuez à nouveau l'envoi afin de recevoir du crédit pour ces éléments.

59. Lorsqu'un message vous y invite, sélectionnez **Oui**.

Après quelques minutes, le volet des niveaux s'affiche et vous montre le nombre de points que vous avez gagné pour chaque tâche. Si les résultats ne s'affichent pas après quelques minutes, choisissez **Grades** (Niveaux) en haut de ces instructions.

Conseil : vous pouvez envoyer votre travail plusieurs fois. Après avoir modifié votre travail, choisissez à nouveau **Envoyer**. Votre dernier envoi est enregistré pour cet atelier.

60. Afin de trouver des commentaires détaillés sur votre travail, sélectionnez **Submission Report** (Rapport d'envoi).

Conseil : pour toutes les vérifications pour lesquelles vous n'avez pas reçu la totalité des points, le rapport d'envoi contient parfois des détails utiles.

Fin de l'atelier

Félicitations ! Vous avez terminé l'atelier.

61. Choisissez **End Lab** (Terminer l'atelier) en haut de cette page, puis sélectionnez **Oui** pour confirmer que vous souhaitez terminer l'atelier.

Un volet s'affiche avec le message *You may close this message box now...* (Vous pouvez fermer cette boîte de message maintenant...)

62. Cliquez sur **X** dans le coin supérieur droit pour fermer le volet.

Conclusion

Félicitations ! Vous avez réussi à :

- Explorer les utilisateurs et les groupes IAM pré-créés
- Inspecter les politiques IAM appliquées aux groupes pré-créés
- Suivre un scénario réel, ajouté des utilisateurs à des groupes en activant des capacités spécifiques
- Localiser et utiliser l'URL de connexion IAM
- Tester les effets des politiques sur l'accès aux services