Introdução ao AWS Identity and Access Management (IAM)

Em muitos ambientes de negócios, acesso envolve um único login em um computador ou rede de sistemas de computador que fornece ao usuário acesso a todos os recursos da rede. Esse acesso inclui direitos a pastas pessoais e compartilhadas em um servidor de rede, intranets da empresa, impressoras e outros recursos de rede e dispositivos. Usuários não autorizados podem rapidamente explorar esses mesmos recursos se o controle de acesso e procedimentos de autenticação associados não forem definidos de forma adequada.

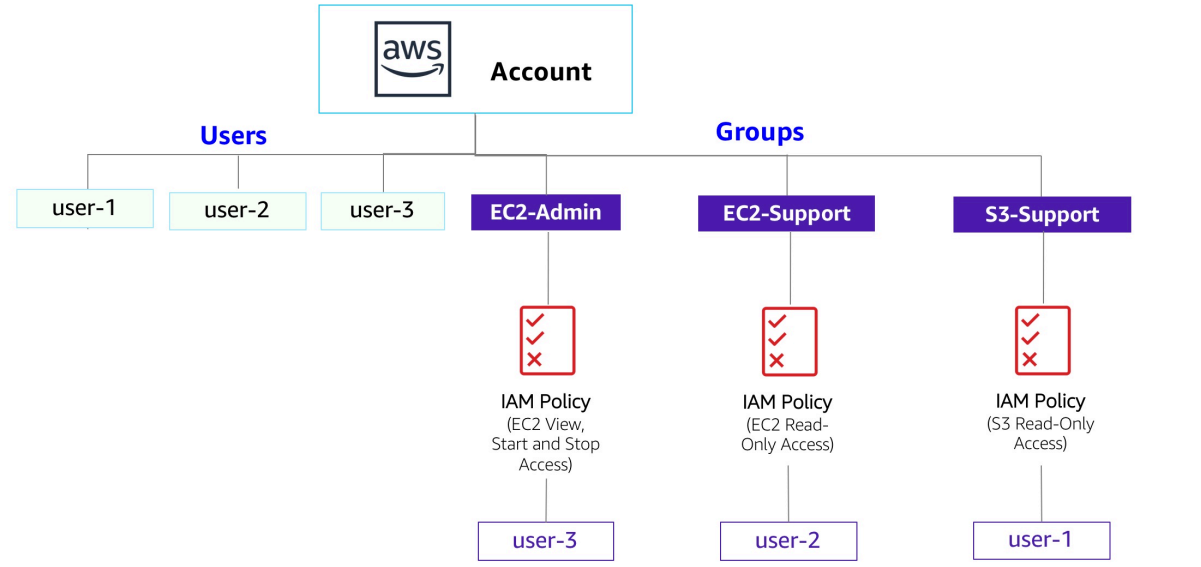
Neste laboratório, você explorará usuários, grupos de usuários e políticas no serviço AWS Identity and Access Management (IAM).

Objetivos

Depois de concluir esse laboratório, você deverá ser capaz de:

- Criar e aplicar uma política de senhas do IAM
- Explorar os usuários e grupos de usuários pré-criados do IAM
- Inspecionar as políticas do IAM aplicadas aos grupos de usuários pré-criados
- Adicionar usuários a grupos com capacidades específicas ativas
- Localizar e usar o URL de login do IAM
- Testar os efeitos das políticas sobre o acesso ao serviço

A seguir, você encontra um diagrama do ambiente atual com os usuários e grupos de usuários do IAM listados.



Outros serviços da AWS

Durante este laboratório, você poderá receber mensagens de erro ao executar ações além das etapas deste laboratório. Essas mensagens não afetarão sua capacidade de concluir o laboratório.

IAM

O IAM pode ser usado para o seguinte:

- **Gerenciar usuários do IAM e o acesso:** você pode criar usuários e atribuir a eles credenciais de segurança individuais (chaves de acesso, senhas e dispositivos de autenticação multifator). É possível gerenciar as

permissões para controlar quais operações um usuário pode executar.

- **Gerenciar funções e as permissões do IAM:** um perfil do IAM é semelhante a um usuário, já que é uma AWS Identity com políticas de permissão que definem o que a identidade pode e não pode fazer na Amazon Web Services (AWS). No entanto, em vez de ser associada exclusivamente a uma pessoa, a finalidade da função é ser assumida por qualquer pessoa que precise dela.
- **Gerenciar usuários federados e as permissões:** você pode ativar a federação de identidades para permitir que os usuários existentes na sua empresa acessem o console de gerenciamento da AWS, chamem as interfaces de programação de aplicativo (APIs) da AWS e acessem recursos, sem precisar criar um usuário do IAM para cada identidade.

Duração

O laboratório levará aproximadamente **60 minutos** para ser concluído.

Acesso ao Console de gerenciamento da AWS

1. No canto superior direito destas instruções, escolha ▸ **Start Lab** (Iniciar laboratório)

   Dica de solução de problemas: se você receber um erro de **Access Denied** (Acesso negado), feche a caixa de erro e escolha ▸ **Start Lab** (Iniciar laboratório) novamente.

2. As informações a seguir indicam o status do laboratório:

   - Um círculo vermelho ao lado de **AWS** 🔴 no canto superior esquerdo desta página indica que o laboratório não foi iniciado.
   - Um círculo amarelo ao lado de **AWS** 🟡 no canto superior esquerdo desta página indica que o laboratório está sendo iniciado.
   - Um círculo verde ao lado de **AWS** 🟢 no canto superior esquerdo desta página indica que o laboratório está pronto.

   Aguarde até que o laboratório esteja pronto para prosseguir.

3. Na parte superior dessas instruções, escolha o círculo verde ao lado de **AWS** 🟢

   Essa opção abrirá o console de gerenciamento da AWS em uma nova guia do navegador. O sistema faz o login automaticamente.

   Dica: se uma nova guia do navegador não for aberta, um banner ou um ícone na parte superior indicará que o navegador está impedindo que o site abra janelas pop-up. Selecione o banner ou ícone e escolha **Allow pop-ups** (Permitir pop-ups).

4. Caso veja uma caixa de diálogo pedindo que você mude para a nova página inicial do console, escolha **Switch to the new Console Home** (Trocar para a nova página inicial do console).

5. Organize a guia do console de gerenciamento da AWS para que ela seja exibida junto com essas instruções. De preferência, deixe as duas guias do navegador abertas para acompanhar as etapas do laboratório.

   ⚠ **Não altere a Região do laboratório, a menos que receba instruções específicas para fazer isso**.

Tarefa 1: criar uma política de senhas para a conta

Nesta tarefa, você criará uma política de senhas para sua conta da AWS. Esta política afeta todos os usuários associados à conta.

6. Primeiro, considere a região em que você está (por exemplo, **Oregon**). Ela é exibida no canto superior direito da página do console.

7. No console de gerenciamento da AWS, na caixa de pesquisa 🔍, insira `IAM` e o selecione.

8. No painel de navegação à esquerda, escolha **Account settings** (Configurações da conta).

Aqui, é possível ver a política de senhas padrão e que está em vigor atualmente. A empresa para a qual você está trabalhando tem requisitos muito mais rígidos e você precisa atualizar esta política.

9. Escolha **Change password policy** (Alterar política de senhas).
10. Em **Select your account password policy requirements** (Selecione os requisitos da política de senhas para sua conta), configure as seguintes opções:
    - Em **Enforce minimum password length** (Defina um comprimento mínimo para a senha), altere `8` para `10` caracteres.
    - Marque todas as caixas de seleção exceto **Password expiration requires administrator reset** (Expiração da senha requer redefinição do administrador).
    - Em **Enable password expiration** (Habilitar expiração de senha), deixe a opção padrão de **90** dias.
    - Em **Prevent password reuse** (Evitar reuso de senha), deixe a opção padrão de **5** senhas.
11. Clique em **Save Changes** (Salvar alterações).

    Essas alterações têm efeito no nível da conta da AWS e se aplicam a todo usuário associado à conta.

Resumo da tarefa 1

Nessa tarefa, você fortaleceu os requisitos de senha criando uma política de senha personalizada. As várias opções de senha que você selecionou agora tornaram as senhas criadas pelos usuários muito mais difíceis de serem descobertas.

Tarefa 2: explorar usuários e grupos de usuários

Nesta tarefa, você explorará os usuários e grupos de usuários que foram criados para você no IAM.

12. No painel de navegação à esquerda, escolha **Users** (Usuários).

    Os seguintes usuários do IAM foram criados para você:

    - user-1
    - user-2
    - user-3
13. Escolha **user-1**.

    Você acessará uma página de **Summary** (Resumo) do **user-1**. A guia **Permissions** (Permissões) será exibida.

    Observe que o user-1 não tem permissões.
14. Escolha a guia **Groups** (Grupos).

    user-1 também não é membro de nenhum grupo de usuários.

    ℹ Um grupo de usuários consiste em vários usuários que precisam de acesso aos mesmos dados. Privilégios podem ser distribuídos para o grupo todo de usuários em vez de apenas para cada indivíduo. Essa opção é muito mais eficaz ao aplicar permissões e dá mais controle geral de acesso a recursos do que aplicar permissões a indivíduos.
15. Selecione a guia **Security credentials** (Credenciais de segurança).

    O user-1 recebe uma **Console password** (Senha do console).
16. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).

    Os seguintes grupos de usuários já foram criados para você:

    - EC2-Admin
    - EC2-Support
    - S3-Support
17. Escolha o grupo **EC2-Support**.

Essa opção exibirá a página **Summary** (Resumo) do grupo **EC2-Support**.

18. Selecione a guia **Permissions** (Permissões).

    Esse grupo tem uma política gerenciada associada a ele, chamada **AmazonEC2ReadOnlyAccess**. As políticas gerenciadas são políticas predefinidas (criadas pela AWS ou pelos administradores) que podem ser associadas a usuários e grupos de usuários do IAM. Quando a política é atualizada, as alterações são imediatamente aplicadas a todos os usuários e grupos de usuários anexados a ela.

19. Ao lado da política **AmazonEC2ReadOnlyAccess**, selecione o sinal de mais para exibi-la.

    Uma política define quais ações são permitidas ou negadas para recursos específicos da AWS. Esta política concede permissão para listar e descrever informações sobre o Amazon Elastic Compute Cloud (EC2), o Elastic Load Balancing (ELB), o Amazon CloudWatch e o Amazon EC2 Auto Scaling. Essa capacidade de visualizar recursos, mas não os modificar, é ideal para ser atribuída a uma função de suporte.

    A seguir, você encontrará a estrutura básica das declarações de uma política do IAM:

    - **Effect** (Efeito) indica se deseja **Allow** (Permitir) ou **Deny** (Negar) as permissões.
    - **Action** (Ação) especifica as chamadas de API que podem ser feitas em um serviço da AWS (por exemplo, *cloudwatch:ListMetrics*).
    - **Resource** (Recurso) define o escopo de entidades cobertas pela regra de política (por exemplo, um bucket específico do Amazon Simple Storage Service [Amazon S3], uma instância do EC2 ou *, que indica *qualquer recurso*).

20. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).
21. Escolha o grupo **S3-Support**.
22. Selecione a guia **Permissions** (Permissões).

    O grupo S3-Support tem a política **AmazonS3ReadOnlyAccess** anexada.

23. Ao lado da política **AmazonS3ReadOnlyAccess**, selecione o sinal de mais para exibi-la.

    Essa política tem permissões para obter e listar recursos no Amazon S3.

24. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).
25. Escolha o grupo **EC2-Admin**.
26. Selecione a guia **Permissions** (Permissões).

    Esse grupo é um pouco diferente dos outros dois. Ao invés de uma política gerenciada, ele tem uma política **Customer inline** (incorporada ao cliente), que é uma política atribuída a apenas um usuário ou grupo. As políticas incorporadas são normalmente usadas para aplicar permissões em situações pontuais.

27. Ao lado da política **EC2-Admin-Policy**, selecione o sinal de mais para exibi-la.

    Essa política concede permissão para visualizar (Describe) informações sobre o Amazon EC2 e para iniciar e interromper instâncias.

Resumo da tarefa 2

Nessa tarefa, você viu os usuários e grupos de usuários pré-criados. Você aprendeu sobre as políticas anexadas aos grupos de usuário e quais as diferenças entre grupos de usuários e as diferenças entre os grupos e suas permissões.

28. Em **Actions** (Ações), clique no link **Show Policy** (Exibir política).

    Uma política define quais ações são permitidas ou negadas para recursos específicos da AWS. Esta política concede permissão para listar e descrever informações sobre o Amazon Elastic Compute Cloud (EC2), o Elastic Load Balancing (ELB), o Amazon CloudWatch e o Amazon EC2 Auto Scaling. Essa capacidade de visualizar recursos, mas não os modificar, é ideal para ser atribuída a uma função de suporte.

    A seguir, você encontrará a estrutura básica das declarações de uma política do IAM:

- **Effect** (Efeito) indica se deseja **Allow** (Permitir) ou **Deny** (Negar) as permissões.
- **Action** (Ação) especifica as chamadas de API que podem ser feitas em um serviço da AWS (por exemplo, *cloudwatch:ListMetrics*).
- **Resource** (Recurso) define o escopo de entidades cobertas pela regra de política (por exemplo, um bucket específico do Amazon Simple Storage Service [Amazon S3], uma instância do EC2 ou *, que indica *qualquer recurso*).

29. Feche a janela **Show Policy** (Exibir política) e selecione a ✖.
30. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).
31. Escolha o grupo **S3-Support**.

    O grupo S3-Support tem a política **AmazonS3ReadOnlyAccess** anexada.
32. Abaixo do menu **Actions** (Ações), clique no link **Show Policy** (Exibir política).

    Essa política tem permissões para obter e listar recursos no Amazon S3.
33. Feche a janela **Show Policy** (Exibir política) e selecione a ✖
34. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).
35. Escolha o grupo **EC2-Admin**.

    Esse grupo é um pouco diferente dos outros dois. Ao invés de uma política gerenciada, ele tem uma política **Customer inline** (incorporada ao cliente), que é uma política atribuída a apenas um usuário ou grupo. As políticas incorporadas são normalmente usadas para aplicar permissões em situações pontuais.
36. Em **Actions** (Ações), escolha **Show Policy** (Exibir política) para visualizar a política.

    Essa política concede permissão para visualizar (Describe) informações sobre o Amazon EC2 e para iniciar e interromper instâncias.
37. Na parte inferior da tela, escolha **Cancel** (Cancelar) para fechar a política.

Resumo da tarefa 2

Nessa tarefa, você viu os usuários e grupos de usuários pré-criados. Você aprendeu sobre as políticas anexadas aos grupos de usuário e quais as diferenças entre grupos de usuários e suas permissões.

Cenário de negócios

No restante deste laboratório, você trabalhará com esses usuários e grupos para ativar permissões no seguinte cenário empresarial:

Sua empresa tem usado mais a AWS e está usando muitas instâncias do Amazon EC2, além de uma grande quantidade de armazenamento do Amazon S3. Você deseja conceder acesso a novos membros da equipe de acordo com as funções de trabalho:

Usuário	No grupo	Permissões
user-1	S3-Support	Acesso somente leitura ao Amazon S3
user-2	EC2-Support	Acesso somente leitura ao Amazon EC2
user-3	EC2-Admin	Visualizar, iniciar e interromper instâncias do EC2

Tarefa 3: adicionar usuários a grupos

Recentemente, você contratou o **user-1** para uma função de suporte ao Amazon S3. Você o adiciona ao grupo **S3-Support** para que ele herde as permissões necessárias por meio da política **AmazonS3ReadOnlyAccess** anexada.

💬 Você pode ignorar todos os erros **not authorized** (não autorizado) que aparecerem durante essa tarefa. Eles são causados porque sua conta de laboratório tem permissões limitadas, mas isso não impede que você finalize o laboratório.

Adicionar user-1 ao grupo S3-Support

38. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).
39. Escolha o grupo **S3-Support**.
40. Escolha a guia **Users** (Usuários).
41. Na guia **Users** (Usuários), selecione **Add users** (Adicionar usuários).
42. Na janela **Add Users to S3-Support** (Adicionar usuários ao S3-Support), configure o seguinte:
    - Marque a caixa de seleção para **user-1**.
    - Escolha **Add Users** (Adicionar usuários).

    Na guia **Users** (Usuários), é possível ver que o user-1 foi adicionado ao grupo.

Adicionar user-2 ao grupo EC2-Support

Você contratou o **user-2** para uma função de suporte ao Amazon EC2.

43. Use o que você aprendeu nas etapas anteriores para adicionar o **user-2** ao grupo **EC2-Support**.

    O user-2 agora deve fazer parte do grupo **EC2-Support**.

Adicionar user-3 ao grupo EC2-Admin

Você contratou o **user-3** como administrador do Amazon EC2 para gerenciar as instâncias do EC2.

44. Use o que você aprendeu nas etapas anteriores para adicionar o **user-3** ao grupo **EC2-Admin**.

    O user-3 agora deve fazer parte do grupo **EC2-Admin**.
45. No painel de navegação à esquerda, selecione **User groups** (Grupos de usuários).

    Cada grupo deve ter um **1** na coluna **Users** (Usuários) referente ao número de usuários de cada grupo.

    Se não houver um **1** ao lado de cada grupo, reveja as instruções acima para garantir que cada usuário seja atribuído a um grupo, conforme mostrado na tabela da seção **Cenário de negócios**.

Resumo da tarefa 3

Nessa tarefa, você adicionou todos os usuários associados aos grupos.

Tarefa 4: fazer login e testar usuários

Nesta tarefa, você testará as permissões de cada usuário do IAM.

46. No painel de navegação à esquerda, escolha **Dashboard** (Painel).

    A seção **AWS Account** (Conta da AWS) inclui um **URL para login de usuários do IAM nesta conta**. O link deve ter o seguinte formato: **https://123456789012.signin.aws.amazon.com/console**

    Você pode usar o link para fazer login na conta da AWS que você está utilizando no momento.
47. Copie o **URL para login de usuários do IAM nesta conta** e cole em um editor de texto.
48. Abra uma janela privada usando as seguintes instruções para seu navegador da web.

    Mozilla Firefox

- Selecione as barras de menu ☰ no canto superior direito da tela.
- Escolha **New Private Window** (Nova janela privada).

Google Chrome

- Selecione a elipse ⋮ no canto superior direito da tela.
- Selecione **New Incognito window** (Nova janela anônima).

Microsoft Edge

- Selecione a elipse ••• no canto superior direito da tela.
- Clique em **New InPrivate window** (Nova janela InPrivate).

Microsoft Internet Explorer

- Clique na opção de menu **Tools** (Ferramentas).
- Selecione **InPrivate Browsing** (Navegação privada).

49. Cole o **URL de login de usuários do IAM nesta conta** na janela privada e pressione Enter.

    Agora, faça login como **user-1**, que foi contratado como parte da equipe de suporte de armazenamento do S3.

50. Faça login com as seguintes credenciais:

    - **IAM user name (Nome de usuário do IAM):** Insira `user-1`
    - **Password (Senha):** Insira `Lab-Password1`

51. Escolha **Sign in** (Fazer login).

    Caso veja uma caixa de diálogo pedindo que você mude para a nova página inicial do console, escolha **Switch to the new Console Home** (Trocar para a nova página inicial do console).

52. No menu **Services** (Serviços), selecione **S3**.

53. Clique no nome de um de seus buckets e navegue pelo conteúdo.

    Como seu usuário faz parte do grupo **S3-Support** no IAM, ele tem permissão para visualizar uma lista de buckets do S3 e todo o conteúdo deles.

    Agora, teste se o usuário consegue acessar o Amazon EC2.

54. No menu **Services** (Serviços), escolha **EC2**.

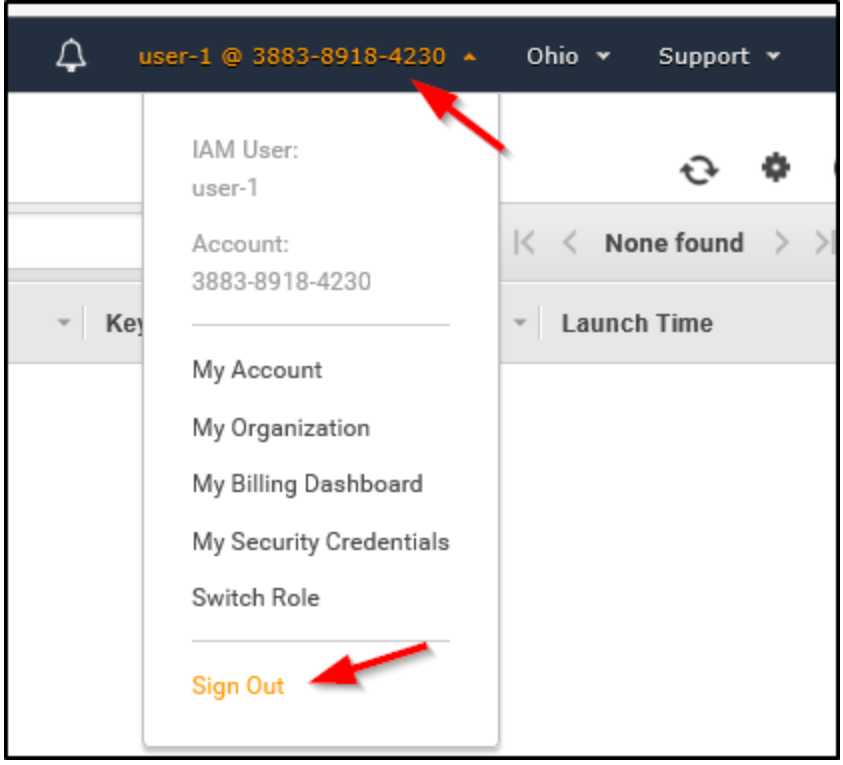
55. No painel de navegação à esquerda, escolha **Instances** (Instâncias).

    Não há nenhuma instância listada. Em vez disso, aparece a seguinte mensagem: **You are not authorized to perform this operation** (Você não tem autorização para realizar essa operação). A mensagem é exibida porque o usuário não recebeu permissões para usar o Amazon EC2.

    Agora, faça login como **user-2**, que foi contratado como responsável pelo suporte do Amazon EC2.

56. Desconecte o user-1 do **console de gerenciamento da AWS** seguindo as etapas a seguir:

    - Na parte superior da tela, selecione **user-1**.
    - Escolha **Sign Out** (Sair).



57. Cole o **URL de login de usuários do IAM nesta conta** na janela privada e pressione Enter.

    Esse link deve estar no seu editor de texto.

58. Faça login com as seguintes credenciais:

    - **IAM User name (Nome de usuário do IAM):** insira `user-2`
    - **Password (Senha):** insira `Lab-Password2`

59. Escolha **Sign in** (Fazer login).

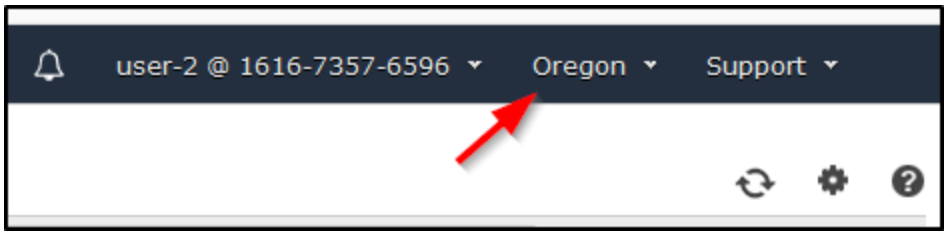
    Caso veja uma caixa de diálogo pedindo que você mude para a nova página inicial do console, escolha **Switch to the new Console Home** (Trocar para a nova página inicial do console).

60. No menu **Services** (Serviços), escolha **EC2**.

61. No painel de navegação à esquerda, escolha **Instances** (Instâncias).

    Agora, você consegue ver uma instância do EC2 porque tem permissões de somente leitura. No entanto, você não consegue fazer nenhuma alteração nos recursos do Amazon EC2.

    ⚠Se você não conseguir ver uma instância do EC2, talvez sua região esteja incorreta. No canto superior direito da tela, escolha o menu **Region** (Região) e selecione a região que você anotou no início do laboratório (por exemplo, **Oregon**).

    A instância do EC2 deve estar selecionada . Se não estiver, escolha .

62. Na lista suspensa **Instance state** (Estado da instância), escolha **Stop instance** (Interromper instância).

63. Na janela **Stop instance?** (Interromper instância?), escolha **Stop** (Interromper).

Você recebe um erro que diz, **Failed to stop the instance (Falha ao interromper a instância). Você não tem autorização para realizar essa operação**. Essa mensagem demonstra que a política lhe dá permissão apenas para visualizar as informações, não para alterá-las.

64. Na janela **Stop Instances** (Interromper instâncias), clique em **Cancel** (Cancelar).

    Depois, verifique se o user-2 pode acessar o Amazon S3.

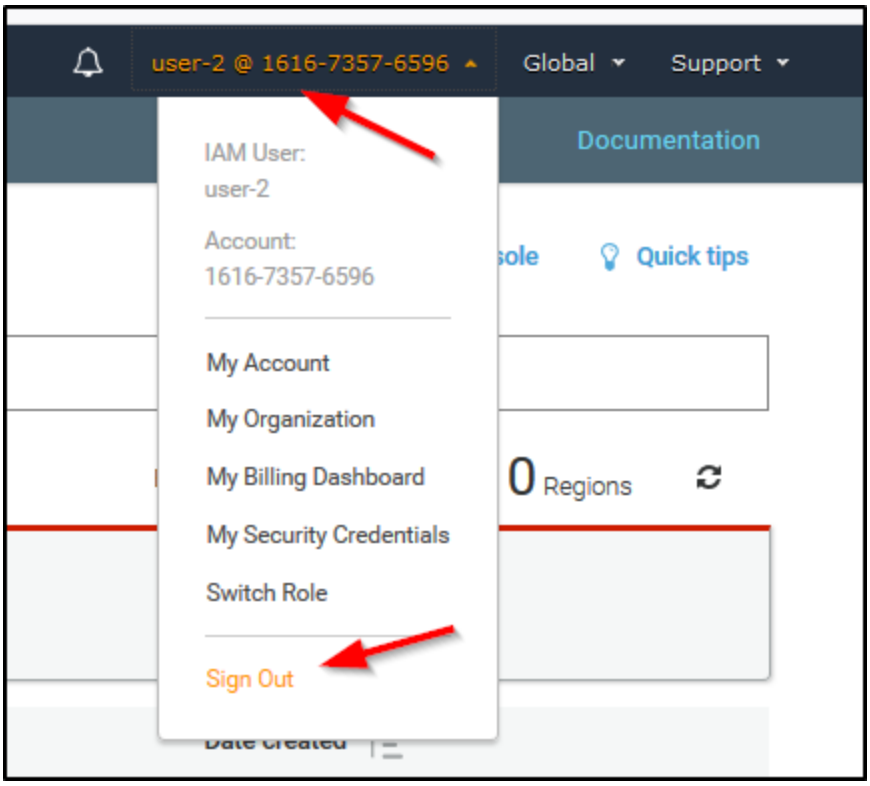
65. No menu **Services** (Serviços), selecione **S3**.

    Você recebe a mensagem **You don't have permissions to list buckets** (Você não tem permissões para listar buckets) porque o user-2 não tem permissões para usar o Amazon S3.

    Agora, faça login como **user-3**, que foi contratado como administrador do Amazon EC2.

66. Desconecte o user-2 do **console de gerenciamento da AWS** seguindo as etapas a seguir:

    - Na parte superior da tela, selecione **user-2**.
      *Escolha **Sign Out** (Sair).



67. Cole o **URL de login de usuários do IAM nesta conta** na janela privada e pressione Enter.

    Se o link não estiver na área de transferência, copie-o do editor de texto no qual você o colou anteriormente.

68. Faça login com as seguintes credenciais:

    - **User name (Nome de usuário):** insira `user-3`

- **Password (Senha):** insira `Lab-Password3`

69. Escolha **Sign in** (Fazer login).

    Caso veja uma caixa de diálogo pedindo que você mude para a nova página inicial do console, escolha **Switch to the new Console Home** (Trocar para a nova página inicial do console).

70. No menu **Services** (Serviços), escolha **EC2**.

71. No painel de navegação à esquerda, escolha **Instances** (Instâncias).

    Como administrador do EC2, agora você deve ter permissões para interromper a instância do EC2.

    A instância do EC2 deve estar selecionada . Se não estiver, escolha .

    ⚠ Se você não conseguir ver uma instância do EC2, talvez sua região esteja incorreta. No canto superior direito da tela, escolha o menu **Region** (Região) e selecione a região que você anotou no início do laboratório (por exemplo, **Oregon**).

72. Na lista suspensa **Instance state** (Estado da instância), escolha **Stop instance** (Interromper instância).

73. Na janela **Stop instance?** (Interromper instância?), escolha **Stop** (Interromper).

    A instância entrará no estado **Stopping** (Interrompendo) e será desligada.

74. Feche a janela privada.

Resumo da tarefa 4

Nessa tarefa, você conseguiu fazer login com os três usuários. Você viu que o user-1 conseguiu visualizar buckets do S3, mas não instâncias do EC2. Depois, você fez login como user-2 e verificou que ele conseguia visualizar instâncias do EC2, mas não parar a instância. O user-2 também não conseguia ver buckets do S3. Depois de fazer login como user-3, você conseguiu visualizar instâncias do EC2 e realizar a ação de interrupção da instância.

Conclusão

🏁 Parabéns! Você concluiu com êxito as seguintes tarefas:

- Criar e aplicar uma política de senhas para IAM
- Explorar usuários e grupos de usuários do IAM pré-criados
- Inspecionar as políticas do IAM aplicadas aos grupos de usuários pré-criados
- Adicionar usuários a grupos com capacidades específicas ativas
- Localizar e usar o URL de login do IAM
- Testar os efeitos das políticas sobre o acesso ao serviço.

Laboratório concluído

75. Escolha ■ **End Lab** (Encerrar laboratório) na parte superior da página e selecione **Yes** (Sim) para confirmar que você deseja encerrar o laboratório.
76. A mensagem **Ended AWS Lab Successfully** (Encerramento bem-sucedido do laboratório da AWS) é exibida rapidamente, indicando que o laboratório foi encerrado.

Para mais informações a respeito do AWS Training and Certification, consulte AWS Training and Certification.

Seu feedback é sempre bem-vindo e valorizado.

Se você quiser compartilhar sugestões ou correções, forneça os detalhes em nosso Formulário de contato do AWS Training and Certification.