Troubleshooting - IAM Access Issues

**SPL-TF-200-SITIAI-1 - Version 1.0.2**

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

This lab demonstrates the concepts of assuming an AWS Identity and Access Management (IAM) role from the Management Console.

As a member of the cloud team at AnyCompany, your company requires that all users who need access to AWS must not have the IAM permissions attached directly to their users identities. Instead, the users permissions only allow them to assume an IAM role which has the required permissions. The company’s policy also requires that least privilege concepts are strictly applied where possible.

The lab is based on a break/fix scenario where you are presented with a problem of a user failing to switch roles from the Management Console. You need to troubleshoot and fix the issue.

High-level guidance and references are provided to assist in fixing the issue. The detailed solution instructions are provided in a hidden collapsible section which you can expand.

OBJECTIVES

By the end of this lab, you will be able to do the following:

* View and update IAM permissions of a user identity-based policy to allow the user to assume an IAM role.
* View and update IAM role trust policy to allow a user to assume an IAM role.
* Apply least privilege concepts.
* Verify the solution.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should have a basic knowledge of:

* Navigating through the AWS Management Console.
* AWS Identity and Access Management (IAM).

DURATION

This lab requires approximately *60* minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

* **Note:** A hint, tip, or important guidance.
* **Hint:** A hint to a question or challenge.
* **Caution:** Information of special interest or importance (not so important to cause problems with the equipment or data if you miss it, but it could result in the need to repeat certain steps).
* **Knowledge check:** An opportunity to check your knowledge and test what you have learned.
* **Answer:** An answer to a question or challenge.

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

 You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

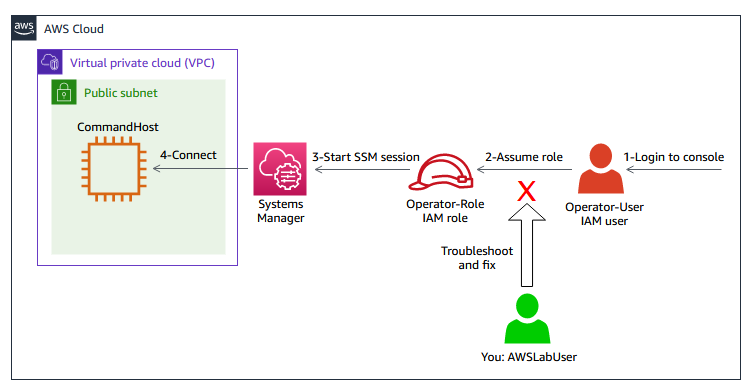
**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

LAB ENVIRONMENT

The following diagram shows the lab scenario:



*Image description: The following list details the major resources in the lab:*

* *An IAM user named****Operator-User****.*
* *An IAM role named****Operator-Role****which need to be assumed by the****Operator-User****.*
* *An Amazon Elastic Compute Cloud (Amazon EC2) instance named****CommandHost****.*
* *Session Manager, a capability of AWS Systems Manager to allow connecting to the EC2 instance.*
* *An IAM user****AWSLabUser****. This is how you can login to the console to troubleshoot and fix the issue.*

**Lab scenario**

A new user **Operator-User** is starting in the company and need access to AWS. The user have been given access to the console. The user is also have been given the following instructions on how to perform his/her duties on AWS:

* Login to the AWS Management Console with the provided **Operator-User** credentials.
* Switch to an IAM role (assume role) named **Operator-Role** using the AWS Management Console.
* Once the role is assumed, start a Systems Manager session to connect to the **CommandHost** instance.
* Run some required scripts from the **CommandHost** prompts.

As a member of the cloud team, you receive a complain that the **Operator-User** is logging to the AWS Management Console but failing to assume the assigned IAM role. Hence, the user is unable perform the duties of his/her role. Your task is to troubleshoot the issue and fix it while applying least privilege concepts in your solution.

AWS SERVICES NOT USED IN THIS LAB

AWS service capabilities used in this lab are limited to what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

**Task 1: Accessing the lab**

In this task, you are introduced on how to access the lab using the **Operator-User** IAM user and how to attempt switching roles to assume the **Operator-Role** IAM role.

When you followed the instructions in the **Start lab** section, you are logged to the console with the **AWSLabUser**. This is the user representing the cloud team member who needs to troubleshoot and fix the issue.

You also need to access the AWS Management Console as the **Operator-User** who is not able to assume the role. You can use this access to reproduce the issue of the user and also to verify the solution after you remediate the issue.

1. In your preferred browser, open a new Private, Incognito, or InPrivate window.
2. Copy the **ConsoleAccessURL** value that is listed to the left of these instructions. Paste the URL into the new web browser window you just opened and press **Enter**.
3. In the **Sign in as IAM user** page:

* For **IAM user name**, enter

Operator-User

.

* For the **Password**, paste the **OperatorUserPassword** value listed to the left of these instructions.
* Choose **Sign in**.

You are logged in to the Console Home page as the **Operator-User**.

Now, you assume the **Operator-Role** IAM role from the AWS Management Console to verify the user issue.

1. At the upper-right corner of the page, choose the **Operator-User** drop-down menu, and then choose **Switch role**.
2. If you are presented with a **Switch role** page that has a **Get started in 3 simple steps** section, then choose **Switch Role**.
3. On the **Switch Role** page:

* For **Account**, copy and paste the **AWSAccountID** value listed to the left of these instructions.
* For **Role**, enter

Operator-Role

.

* For **Display Name**, leave blank as this is just a descriptive name.

1. Choose **Switch Role**.

The following message is displayed *Invalid information in one or more fields. Check your information or contact your administrator.* This indicates that the role switch is not successful and confirms the user issue.

You can re-visit this section whenever you need guidance on how to login as the **Operator-User** and switch roles to assume the **Operator-Role** IAM role.

 Congratulations! You are now familiar with accessing the lab using the **Operator-User** IAM user and attempting to switch roles to assume the **Operator-Role** IAM role.

**Task 2: Troubleshooting and remediating the issue and verifying the solution**

In this task, you attempt to troubleshoot and remediate the issue preventing the **Operator-User** from assuming the **Operator-Role**. You also verify the solution.

After you confirmed the user issue in the previous task, you need to switch back to the browser tab of the console logged with the **AWSLabUser** user to troubleshoot and remediate the issue. The **AWSLabUser** has the required permissions to solve the issue.

1. Choose the AWS Management Console browser tab which has the **AWSLabUser** at the upper-right corner of the page to troubleshoot and remediate the **Operator-User** issue.

Your solution should allow the **Operator-User** to assume the **Operator-Role** successfully and also should strictly adhere to the following least privilege guidelines:

* The **Operator-User** has the permissions to **only** assume the **Operator-Role**.
* The **Operator-Role** can **only** be assumed by the **Operator-User**.

**Hint:**

* You are not allowed to create new identity-based policies. However, you can use pre-configured customer managed policies. The pre-configured policies names you are allowed to use starts with **IAM-User-Policy**.
* If you get denied access when attempting to solve the issue, this means you do not have enough permissions and hence you need to solve the issue using a different way.

DO IT YOURSELF

**Hint:** Here are some references to assist you in solving the issue:

* [Using IAM roles](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html).
* [Troubleshooting IAM roles](https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_roles.html#troubleshoot_roles_cant-assume-role).
* [How to use trust policies with IAM roles](https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/).

**Note:** While navigating through the IAM console pages, you may get a message at the bottom of some IAM console pages indicating that **You need permissions** for some access-analyzers actions. You can ignore this error safely as it is not required to complete the lab.

SOLUTION

Expand the *Detailed instructions* below for the full solution.

**Detailed instructions**

VERIFY THE SOLUTION

Now, verify the solution and check how strictly you applied least privilege concepts.

1. Choose the AWS Management Console browser tab which has the **Operator-User** user at the upper-right corner of the page to attempt assuming the **Operator-Role** role.
2. At the upper-right corner of the page, choose the **Operator-User** drop-down menu, and then choose **Switch role**.
3. If you are presented with a **Switch role** page that has a **Get started in 3 simple steps** section, then choose **Switch Role**.
4. On the **Switch Role** page:

* For **Account**, copy and paste the **AWSAccountID** value listed to the left of these instructions.
* For **Role**, enter

Operator-Role

.

* For **Display Name**, leave blank as this is just a descriptive name.

1. Choose **Switch Role**.

**Note:** If the following message is displayed *Invalid information in one or more fields. Check your information or contact your administrator.* This indicates that the role switch is not successful and the problem is not solved. Try troubleshooting and remediating the issue again.

If your solution is correct, you are redirected to the Console Home page and you can note that the logged entity is the **Operator-Role** at the upper-right corner of the page.

This indicates that you solved the issue. However, you still need to check if you applied least privilege concepts in your solution. You need to connect to the **CommandHost** instance and run a verification script.

1. Copy the **CommandHostSessionURL** value that is listed to the left of these instructions. Paste the URL into a new browser tab and press **Enter** to access the command host terminal.

A validation script runs automatically and displays the results based on the following scoring criteria:

* The total maximum score is 100.
* You score 50 for successfully assuming the role.
* You also get a score of (0-50) based on how strictly your solution follows least privilege concepts.

**Note:** The scoring calculated by the validation script resides inside the temporary lab environment, and hence is not persistent.

The validation script provides a description on which parts of the solution did not follow least privilege concepts.

If your solution does not strictly follows least privilege concepts, you can retry troubleshooting and remediating the related policies.

* **Caution:** If you ran the validation script and decided to retry the solution, you must follow the steps below before attempting remediating the policies. Otherwise, the script might give inaccurate assessment:
* Close the Session Manager browser tab.
* Choose the AWS Management Console browser tab which has the **Operator-Role** at the upper-right corner of the page.
* At the upper-right corner of the page, choose the **Operator-Role** drop-down menu, and then choose **Switch back**. This ensures that you return the console page with the **Operator-User** at the upper-right corner of the page.
* Return to **Task 2** and retry fixing the issue.

 Congratulations! You have successfully remediated the IAM issue preventing the user from assuming the role and verified your solution by assuming the role. You also verified how your solution complies with least privilege concepts.

**Conclusion**

 Congratulations! You have now successfully:

* Viewed and updated IAM permissions of a user identity-based policy to allow the user to assume an IAM role.
* Viewed and updated IAM role trust policy to allow a user to assume an IAM role.
* Applied least privilege concepts.
* Verified the solution.

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

**Additional resources**

* [Digital Course: Introduction to AWS Identity and Access Management (IAM)](https://explore.skillbuilder.aws/learn/course/external/view/elearning/120/introduction-to-aws-identity-and-access-management-iam).
* [Digital Course: AWS Identity and Access Management (IAM) - Troubleshooting](https://explore.skillbuilder.aws/learn/course/external/view/elearning/15564/troubleshooting-aws-identity-and-access-management-iam).
* [Digital Course: Deep Dive with Security: AWS Identity and Access Management (IAM)](https://explore.skillbuilder.aws/learn/course/external/view/elearning/104/deep-dive-with-security-aws-identity-and-access-management-iam).
* [Lab: Introduction to AWS Identity and Access Management (IAM)](https://explore.skillbuilder.aws/learn/course/external/view/elearning/880/introduction-to-aws-identity-and-access-management-iam).

For more information about AWS Training and Certification, see [*https://aws.amazon.com/training/*](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*  
If you would like to share any feedback, suggestions, or corrections, please provide the details in our [*AWS Training and Certification Contact Form*](https://support.aws.amazon.com/#/contacts/aws-training).