



AZ-104 LAB [A] REPORT [WEEK #4]

BY

EMMANUEL MUTURIA™

ADMISSION NUMBER
[ADC-SE02-25011]

TABLE OF CONTENTS

INTRODUCTION.....

TASK #1 [Implement Management Groups].....

TASK #2 [Review and assign a built-in Azure role].....

TASK #3 [Create a custom RBAC role].....

TASK #4 [Monitor role assignments with the Activity Log].....

CONCLUSION.....

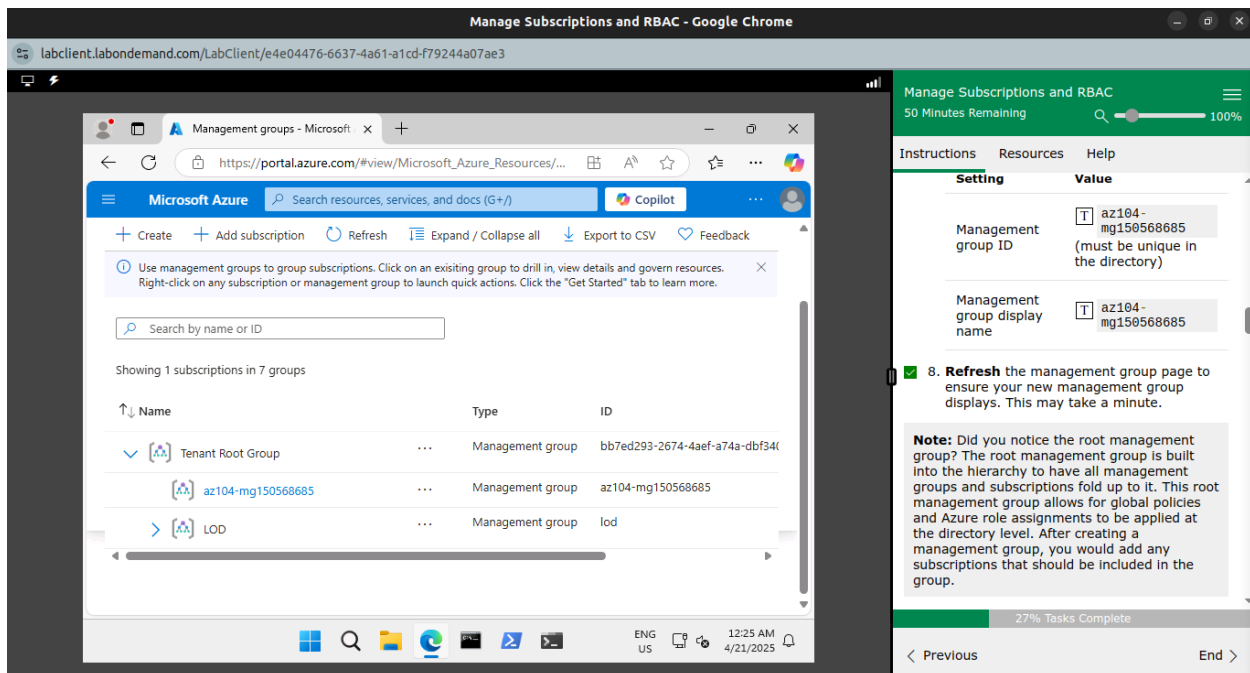
REFERENCES.....

INTRODUCTION

This report documents my completion of the Manage Subscriptions and RBAC AZ-104 Lab. I learnt about Role-Based Access Control [RBAC] and how to use permissions and scopes to control what actions identities can and cannot perform. You also learn how to make subscription management easier using management groups. It contains screenshots and links to the badges to prove the completion of the learning path's modules.

TASK #1 [I !"# #\$% M&\$&'# #\$% ()*+!,]

In this task, I created and configured management groups. Management groups are used to logically organize and segment subscriptions. They allow for RBAC and Azure Policy to be assigned and inherited to other management groups and subscriptions. For example, if your organisation has a dedicated support team for Europe, you can organise European subscriptions into a management group to provide the support staff access to those subscriptions (without providing individual access to all subscriptions). In our scenario everyone at the Help Desk will need to create a support request across all subscriptions.



The screenshot shows the Microsoft Azure portal interface. The main window displays the 'Management groups' page, showing a list of management groups. The table lists the following groups:

Name	Type	ID
Tenant Root Group	Management group	bb7ed293-2674-4aef-a74a-dbf34t
az104-mg150568685	Management group	az104-mg150568685
LOD	Management group	lod

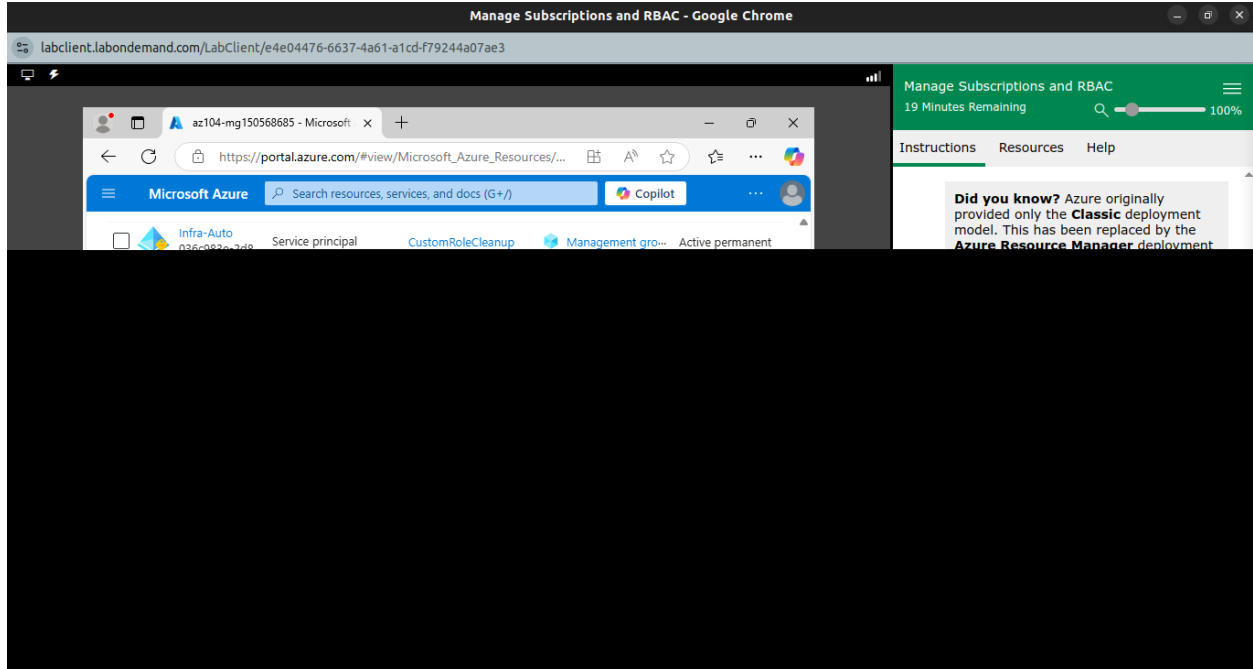
On the right side, there is a task list titled 'Manage Subscriptions and RBAC' with a progress bar at 100%. The task list includes the following instructions:

- 8. **Refresh** the management group page to ensure your new management group displays. This may take a minute.

A note is also present: 'Note: Did you notice the root management group? The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level. After creating a management group, you would add any subscriptions that should be included in the group.'

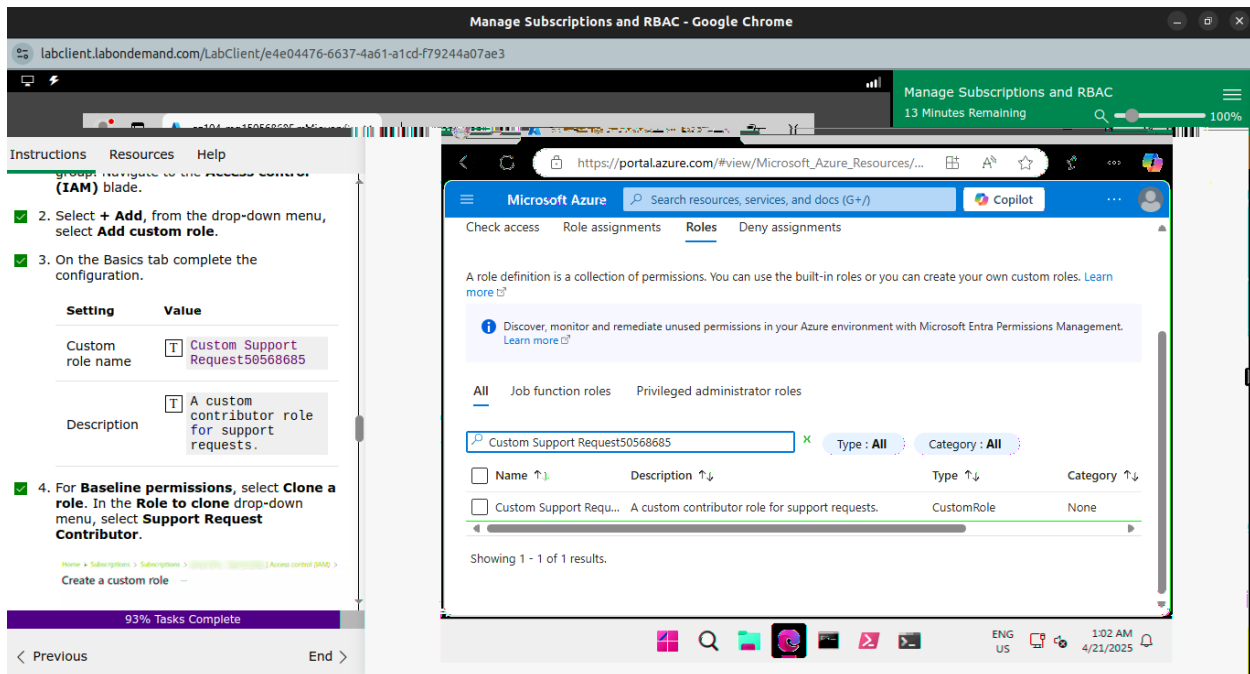
TASK #2 [R#-.# / &\$0 &,,.'\$ & 1+."%-. \$ A2+)#)*"#]

In this task, I reviewed the built-in roles and assign the VM Contributor role to a member of the Help Desk. Azure provides a large number of [built-in roles](#).



TASK #3 [C)## & 4+,%* RBAC)*"#]

In this task, I created a custom RBAC role. Custom roles are a core part of implementing the principle of least privilege for an environment. Built-in roles might have too many permissions for your scenario. I also created a new role and removed permissions that were not necessary.

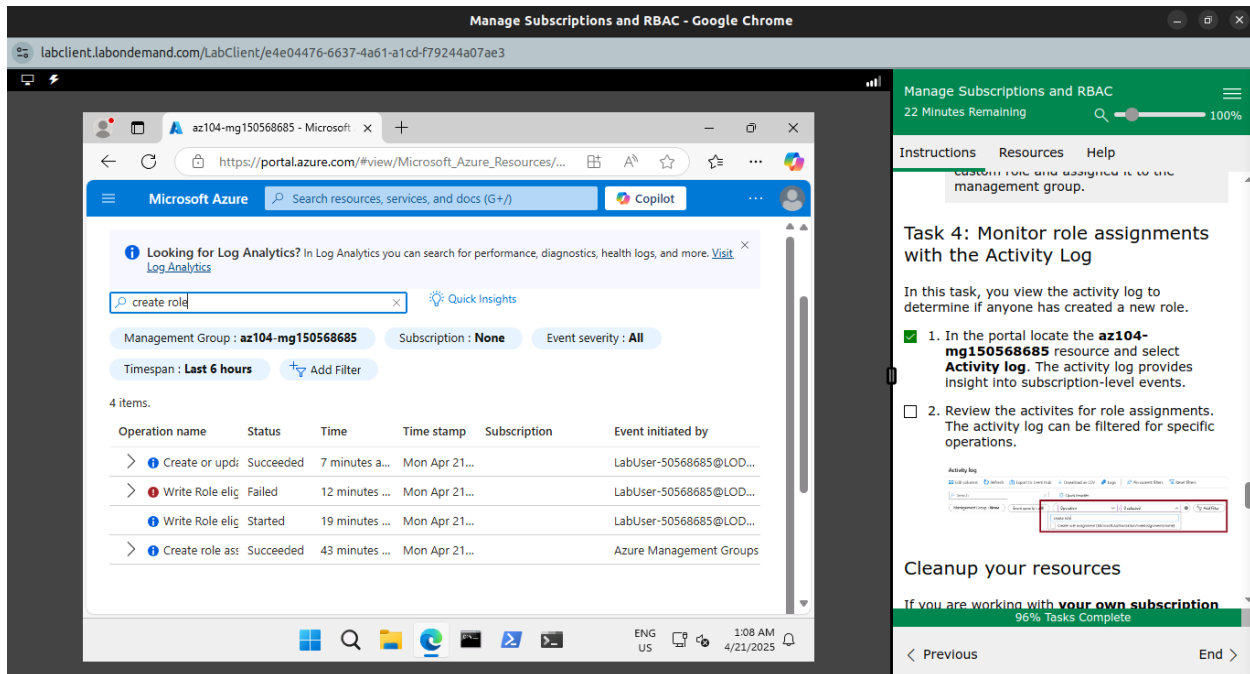


The screenshot displays the Microsoft Azure portal interface for managing subscriptions and RBAC. On the left, a sidebar contains instructions for creating a custom role, including steps for selecting 'Add', completing the configuration, and cloning a role. The main pane shows the 'Roles' tab with a search for 'Custom Support Request50568685'. The search results show a single role with the description 'A custom contributor role for support requests.' and a type of 'CustomRole'.

Name	Description	Type	Category
Custom Support Request50568685	A custom contributor role for support requests.	CustomRole	None

TASK #4 [M*\$.%*))*"# &,,.'\$ #\$\$, /.%5 %5# A4%.-.%6 L*'']

In this task, I viewed the activity log to determine if anyone has created a new role.



Task 4: Monitor role assignments with the Activity Log

In this task, you view the activity log to determine if anyone has created a new role.

1. In the portal locate the **az104-mg150568685** resource and select **Activity log**. The activity log provides insight into subscription-level events.
2. Review the activities for role assignments. The activity log can be filtered for specific operations.

Cleanup your resources

If you are working with your own subscription

96% Tasks Complete

< Previous End >

CONCLUSION

This lab helped solidify the creation and management of roles in Microsoft Entra ID. By practising it, I learnt that Management Groups are used to logically organise subscriptions, the built-in root management group includes all the management groups and subscriptions, Azure has many built-in roles, you can assign these roles to control access to resources, you can create new roles or customise existing roles, roles are defined in a JSON formatted file and include Actions, NotActions, and AssignableScopes, and you can use the Activity Log to monitor role assignments.

REFERENCES

Login - *Skilable TMS.* (2024). Learnondemand.net.
[https://msle.learnondemand.net/Lab/64582?
instructionSetLang=en&classId=676661](https://msle.learnondemand.net/Lab/64582?instructionSetLang=en&classId=676661)