Ghazela Technology Academy

Managing Azure Subscription and Resource Management

We will cover the following topics in this document:

- Azure subscription
- Enterprise agreements subscription
- Subscription support plan
- Creating a free Azure subscription
- Global administrator permission
- Resources group
- Cost management
- Azure subscription policy
- Azure quota and resource tagging
- Management group

1- Azure subscriptions

Azure subscriptions are a collection of resources known as **billing containers**. Each subscription has a unique ID that has been generated by MS automatically while creating the Azure subscription.
If you need to create or access the resources, then you need a subscription access. Without the subscription access, you will not be able to access the resources under Azure subscription.

Let's take a look at the different types of subscriptions:

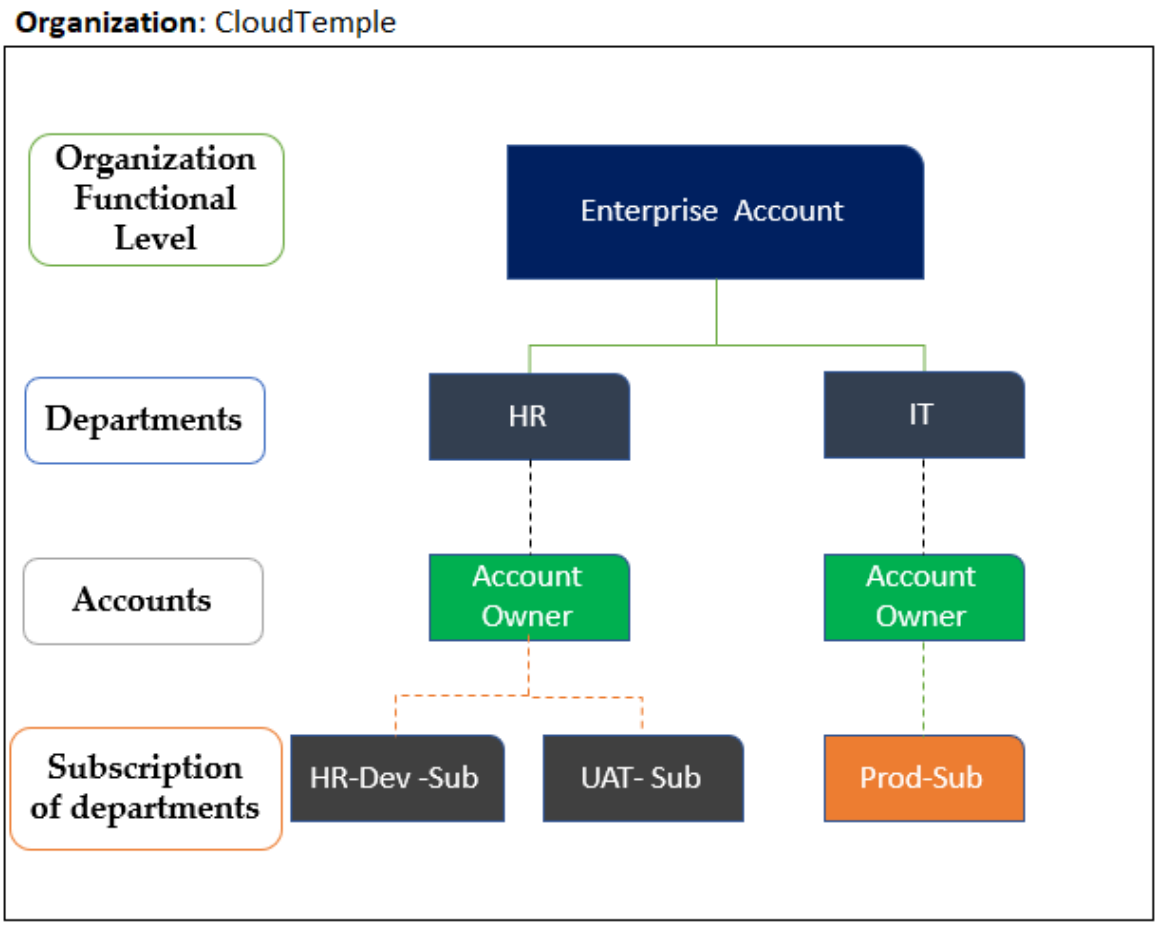
Free subscription	MS provides this subscription. It is free for the first 30 days which includes $230 credit and free 25 services for 12 months. It is used for practical and learning purposes.
Pay-as-you-go subscription	It is used widely in organizations and the pay-as-you-go subscription has a flexible payment method, and there is no limit for purpose or commitments. If a customer wants to cancel the subscription, he/she can cancel the subscription.
Microsoft resellers (Cloud solution provider - CSP)	The CSP subscription is used only at the organization level where MS provides you with the access to work with partners directly to design and implement the solutions to meet your project requirements.
Open	This subscription provides you with the flexibility to work with the same vendor from where you purchased the open volume license program and activated your Azure subscription.
Azure government customer	This subscription is used for US government entities that are eligible to use Azure government services, and they can use the pay-as-you-go service.
Azure Germany customers	This subscription is used for European Union or EFTA entities that are eligible to use Azure government services and they can use the pay-as-you-go service.

1.1- Enterprise agreement subscription:

The EA (Enterprise Agreement) is designed for organizations, and in this subscription, the customer has to sign an agreement with Microsoft directly with the amount of consumption on your Azure resources.
When an organization signs up for the EA agreement, a billing account is created and the billing can be done monthly, quarterly, or yearly based on the agreement.

Enterprise	It is most commonly known as Enterprise agreement, and it is only used by organizations. The EA subscription can be accessed from the Enterprise portal (https://ea.Azure.com) and used to create multiple departments to manage the subscription.
Departments	It is a sub-account of Azure EA subscription where we define the departments and associate a subscription to it, and it can be used by specific departments. We can add multiple departments based on the organizational needs and assign a department owner who can manage the department and subscription under it. It will also help us to add a cap on Azure consumption and based on the subscription utilization, we can decide the monthly or yearly budget.
Accounts	Accounts can be created by a different department and an account administrator can add new accounts to their departments to provide them access to the Azure account. Even an account administrator can create the subscription as well.
Subscriptions	As defined in the Azure subscription level, the subscription is

	a billing container, and all the billing for consumed resources happens at the subscription level. You can set up billing alerts of the budget spent to get an early notification if you have consumed more during a specific period.



1.2- Azure subscriptions support plan

Along with the subscriptions discussed earlier, we can also opt for the following support plan with a subscription which will help you to connect to the MS support team to fix or troubleshoot the issue.

Azure developer support	This kind of subscription support plan is most commonly used for Azure development/testing purposes where MS provides the discounted rates on Azure to support your ongoing development and testing activity.
Professional direct support	This subscription support plan can be used by companies where MS includes its technical, billing, and other teams to get a faster resolution and support.
Standard support	This subscription support plan can be used by companies where MS includes its technical, billing, and other teams to resolve your issues faster with 24/7 support. Most of the companies use this subscription to fix the critical dependence on the Azure subscription

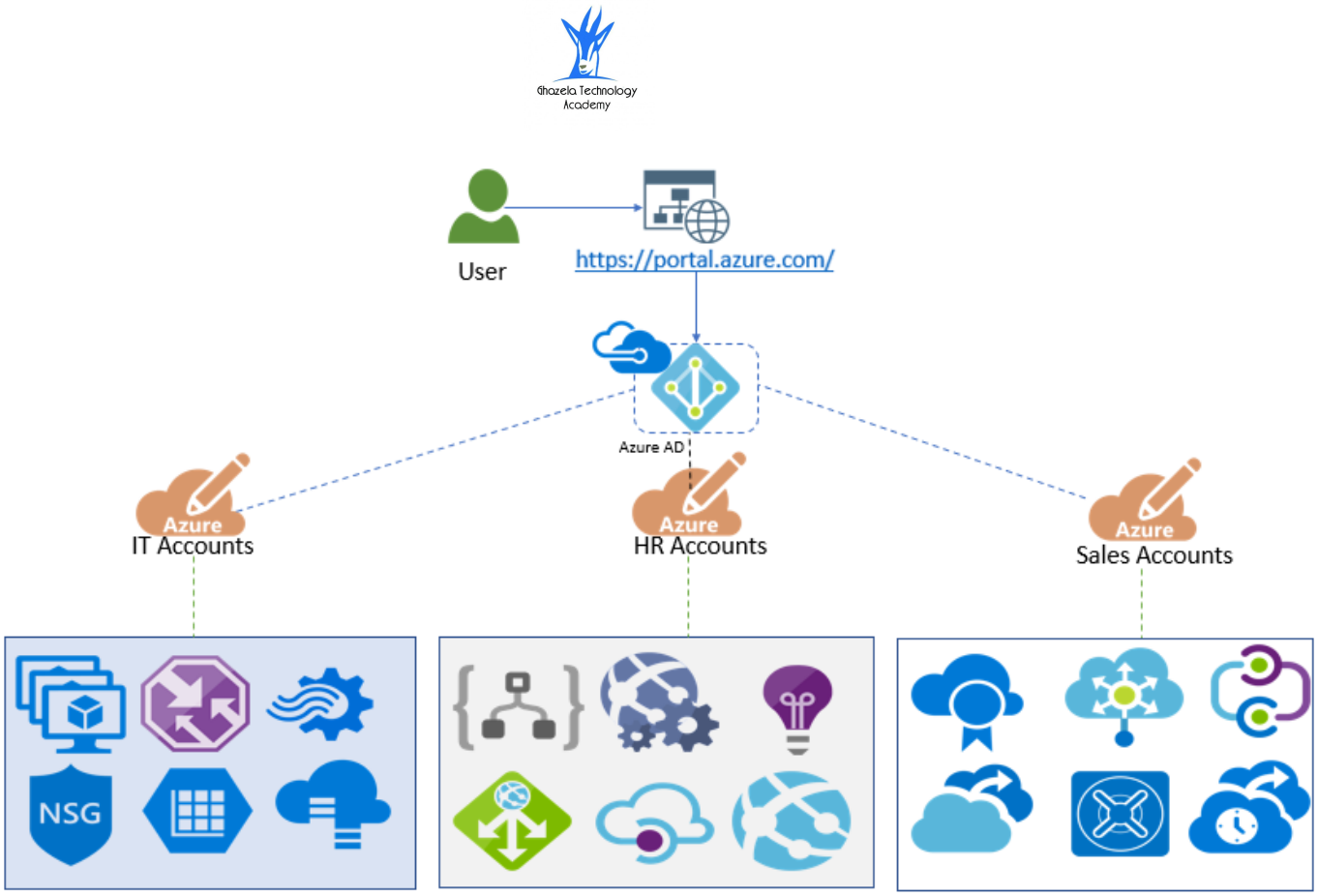
1.3 Azure tenant

An Azure tenant is nothing but Azure AD. It's a dedicated instance of Azure AD that an organization receives and authorizes the users to various cloud services.

An Azure tenant can have multiple subscriptions. However, a subscription cannot have multiple tenants.

In the following diagram, you can see four 3 subscriptions and one directory. All the others are different. Once you create the subscription, the first tenant (Azure AD) will be created, and then the subscription will be associated with it.

If you have a tenant, then you can create multiple subscriptions.



2- Creating a free Azure subscription

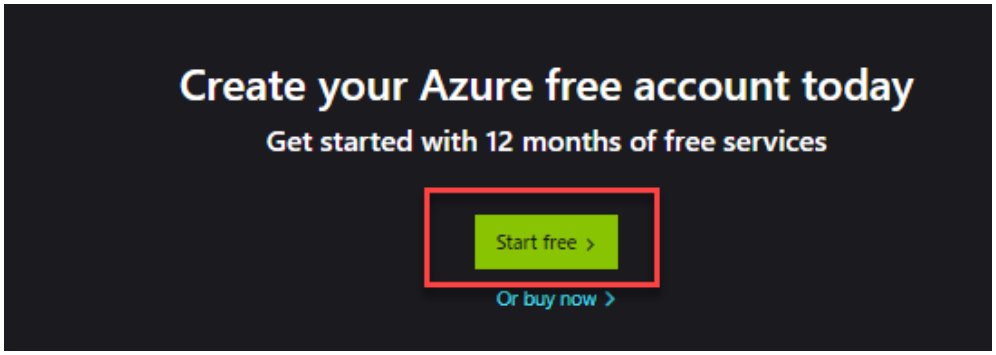
While creating the free subscription, the following benefits are provided by MS Azure:

- 12 months of free popular services
- $200 credit to explore services within 30 days
- 25 services are always free

Step 1:

1. Go to the URL https://Azure.microsoft.com/en-us/free/ .

2. Click on Start free as shown in the following picture:



Step 2:

1. It will ask for your login ID and password.

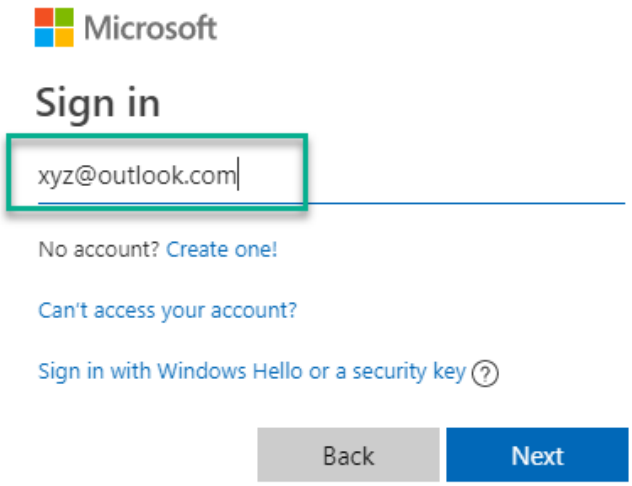
2. Provide your Microsoft ID like (bob@outlook.com, bob@live.com [reference email ID], and so on).

3. You can even log in through your organization ID like gta@mycompany.com.

4. Provide the password for the same.

5. After this, you will be able to log in to the subscriber page.

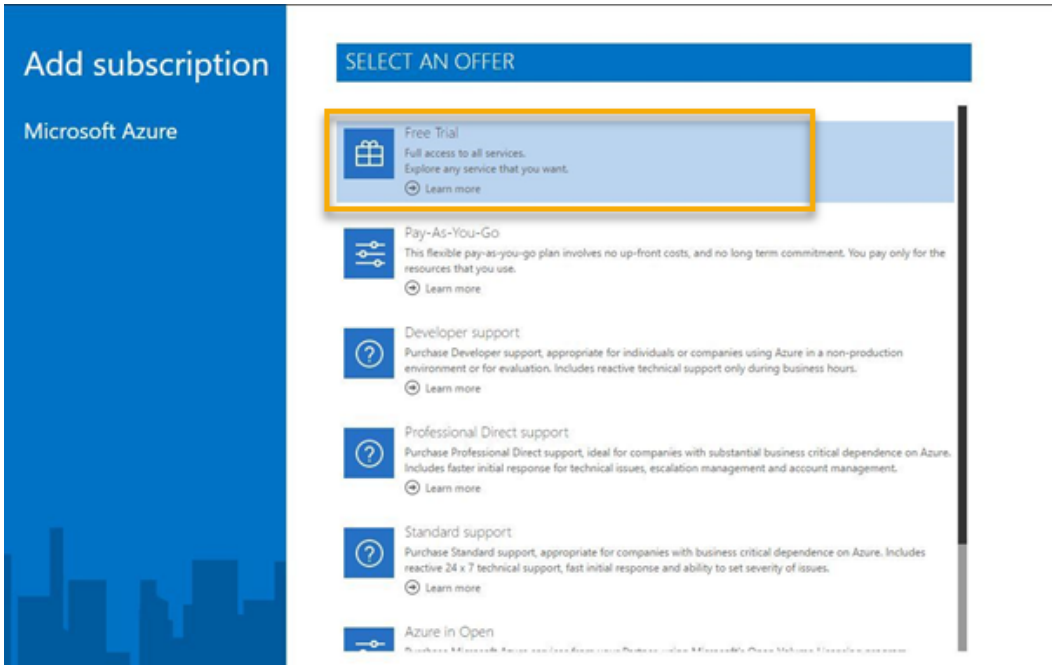
6. Provide your details as shown in the following picture:



Step 3:

1. Click on the free subscription.

2. Select the Free Trial as shown in the following picture:



Step 4:

1. Select the country code.

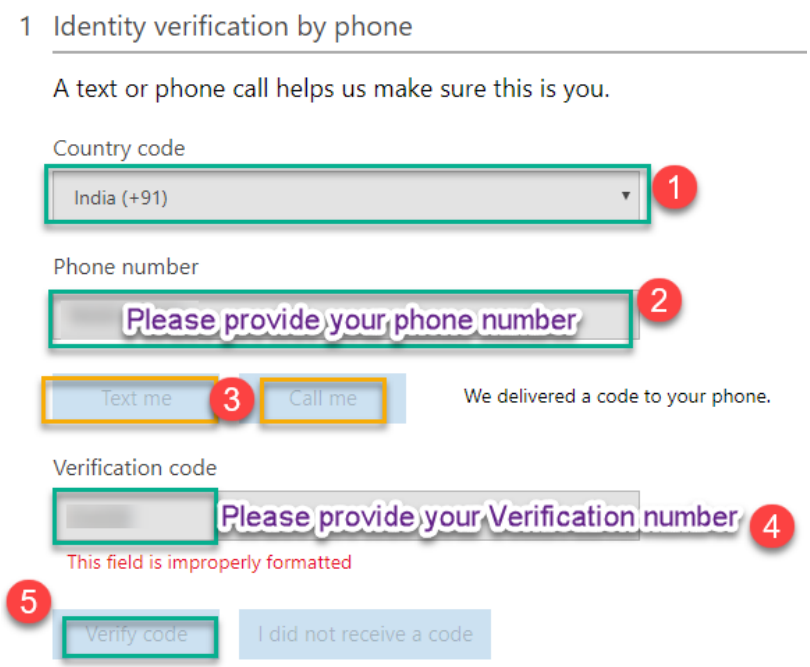
2. Provide the mobile number.

3. Click on Text me or Call me to get the verification code.

4. Once you get the verification code, put it in the Verification code section.

5. Click on the verify code.

6. Once the code is verified, you will be directed to the next tab to fill the payment information.



Step 5:

1. Provide the cardholder name.

2. Enter the card number.

3. Provide the expiry date.

4. Type the CVV number.

5. Provide the address details and click on the Next button.

6. Understand the service usage and click on Next.

7. If you want to add MS support plans, you can do it. (It's chargeable so it's better to not add this plan.)

8. Click on the Agreement section and click on the Signup button.

9. After 10 minutes, you will receive the subscription.

10. Now, you can utilize your subscription and create the services in Azure.

Ghazela Technology Academy

2 Payment Information

Note, we do not accept debit or prepaid cards because they do not support monthly payments in your location. Please use a credit card.

We accept the following cards:

VISA

Cardholder Name

Please provide the card holder name 1

Card number

Please provide the card Number 2

Expires

MM YY 3 Please provide the Expiry Date

CVV 4

Please provide the CVV Number hat's this?

Address line 1

Address line 2 (Optional) 5

Please provide the Address Details

Address line 3 (Optional)

City

State

--Select--

Postal Code

Country/Region

India

Next 6

3 Service Usage Address 7

4 Add technical support 8

5 Agreement 9

Important:

When you create the subscription, make sure you put all the details correctly as this will be used for MS internal purpose.

When you add your card initially, it will charge a minimal amount to verify your credit card and only after that, it will allow you to create the free subscription.

2.1- Global administrator permission

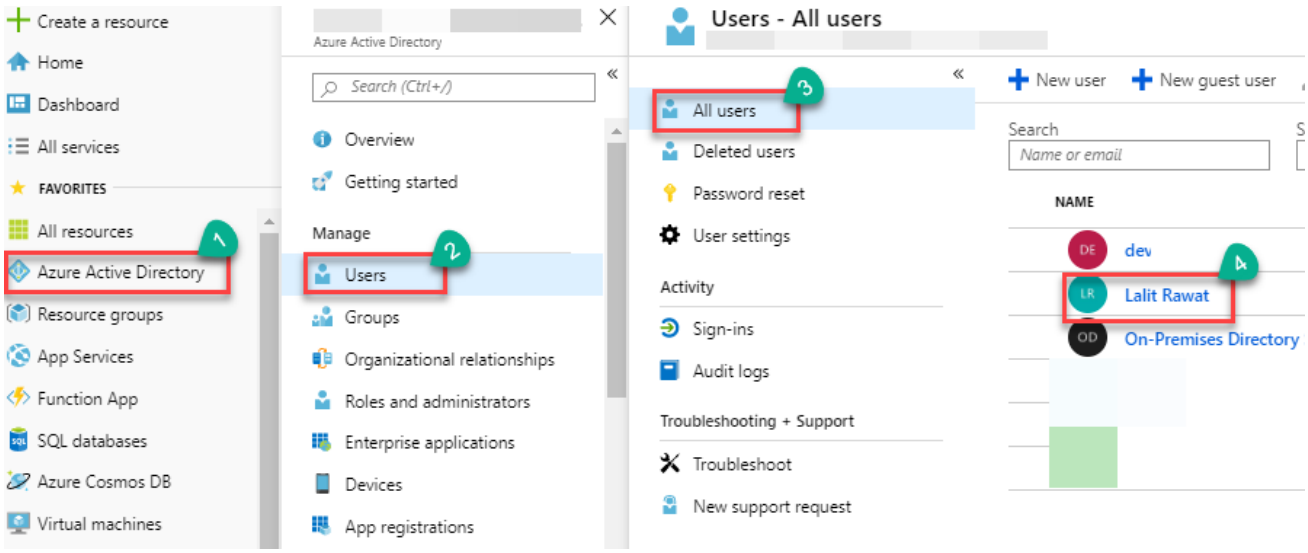
Users who have global administrator permission can access all administrative services like Azure Active Directory, federate services to Azure Active

Directories such as Exchange Online, SharePoint Online, and Skype for Business Online.

The first user ID who signs up for the Azure Active Directory tenant or subscription becomes a global administrator.

Only global administrators can assign other administrator roles. We can have more than one global administrator at the organization level. Global admins can reset the password for users and all other administrators.

1. Click on the Azure Active Directory option.
2. Go to Manage and click on the Users option.
3. Click on All users.
4. Select the user or search the users you want to assign the permission.
5. Select details, as shown in the following picture, for subscription details:



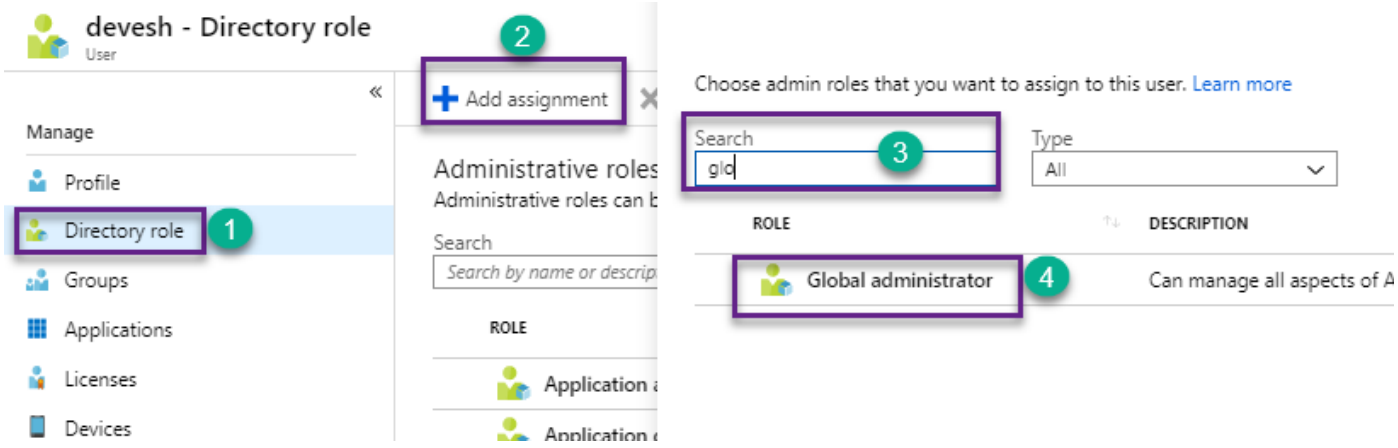
6. Click on the user's name and then click on the Directory role.

7. Then, click on Add assignment.

8. Click on Search and search for a Global administrator role.

9. Select the Global administrator role.

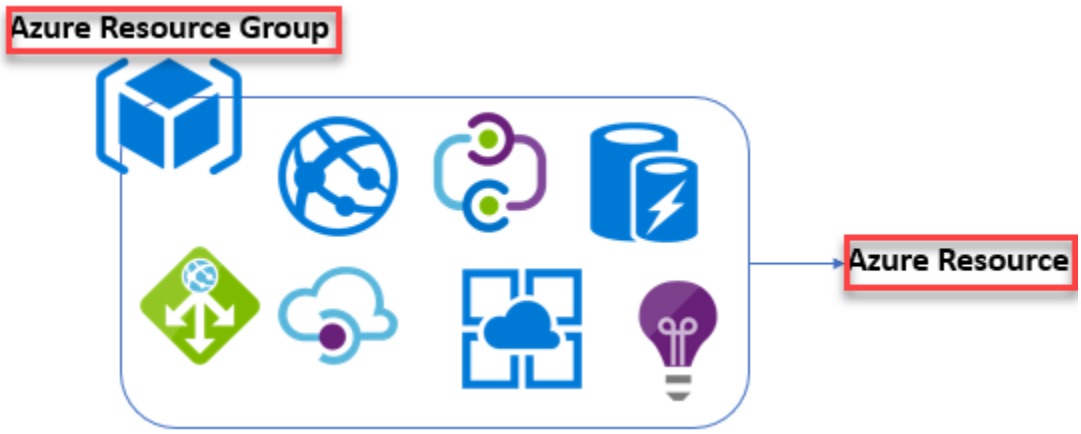
10. Click on the Save button, and your user will have global administrator access. Follow the steps as shown in the following picture:



2.2- Resources group

An Azure resource group is a logical container that contains the Azure resources in it. Resources manage the resources within the resources group together as an entity.

If you have provided the permission to a resource group, then you can also view all the resources which are available in the resource group.

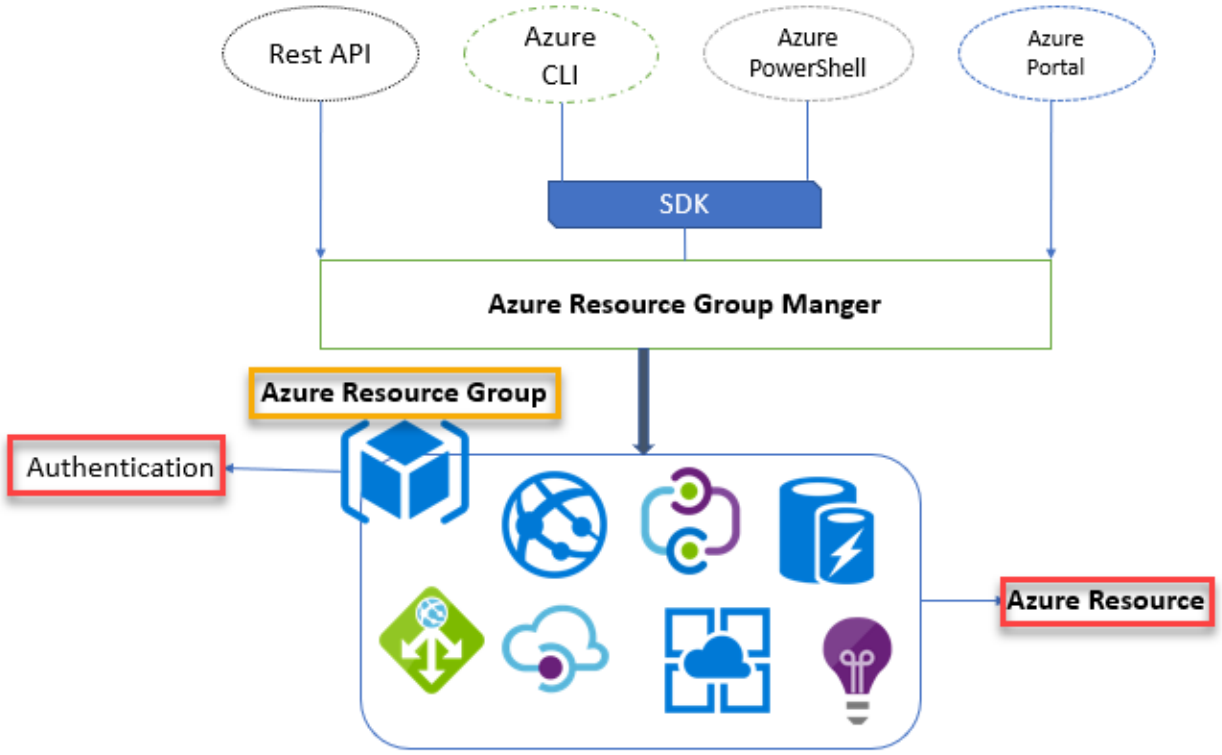


You can even create or delete the resource group. If you delete the resource group, then all the resources which are present in the resource group will be deleted automatically.

2.3- Azure resource group manager

Azure Resource Manager is a deployment and management service for Azure.

It provides management layers that will help to create, update, modify, and delete the resources within the subscription. We can utilize the features like access control, lock, and tag. Refer to the following figure for more details in Azure resource group manager:



3- Cost management

Azure cost management will help you to manage and control your cost.

Organizations can utilize cost management to analyze and manage the cost. It gives you the breakup cost of each resource and resource group. It uses advanced analytics to provide a customized cost to customers.

The cost will be shown based on the consumption of each service and third-party services like Red Hat, Oracle checkpoint firewall, and so on.

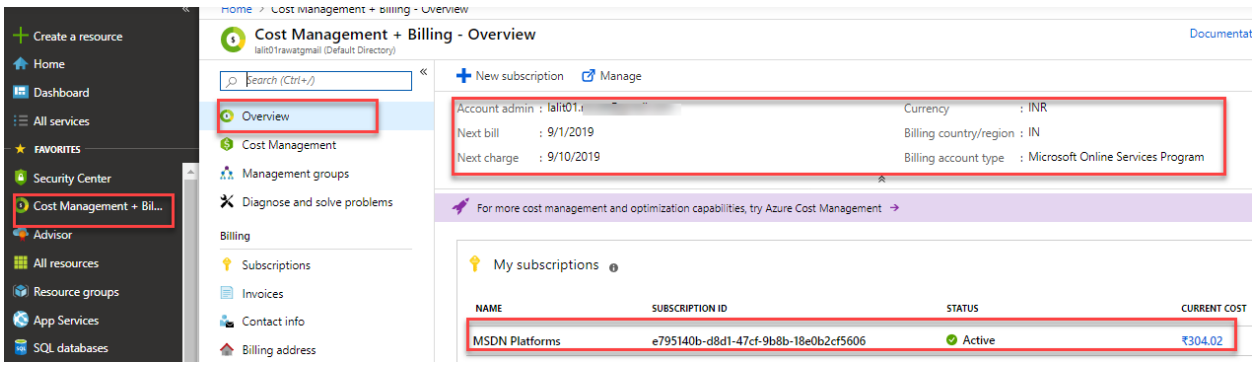
Exploring cost management:

Cost management will add all the subscriptions which are under one tenant. To get the report of each tenant separately, you need to perform the following steps:

1. Click on the **Cost Management + Billing** option from the **FAVORITES** item or search on the Azure portal.

2. Click on **Overview** that will help you to get all the subscription accounts under your tenant.

3. Then, you will be able to view how much you have spent every month. For a detailed analysis, use the cost management tool and follow the steps performed as shown in the following picture:

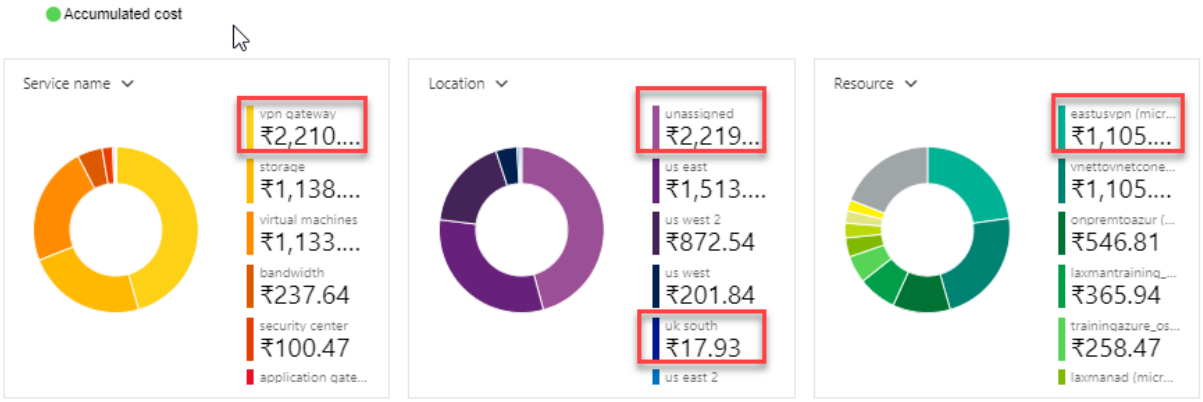


Cost management tools will help you to get more details of resource services costs. It will help you to set up an alert for your Azure account, and you can define the budget as well.

4. Click on Cost analysis:

- You can see the graphical view of the cost analysis.
- You can see the usage of each service, region.
- If you want to go deeper, then click on each resource and you will get more details.
- You can export the data in CSV or Excel file for your reference or telly purpose

- The following screenshot displays a sample report which is shown in cost view models



4.1- Configuration of the budget alerts

The configuration of the budget alerts will help you get the alerts when your subscription cost gets utilized beyond the limit, and you can set an account spending limit as well.

Perform the following steps to configure the budget alerts:

1. Click on the Budgets option in the left pane.

2. Once you click on the budget, you will get a window to provide the information.

3. Provide the alert name or budget name.

4. Reset the period month/years/weeks.

5. Provide the start date and end date of your budget.

6. Provide the number of your budget.

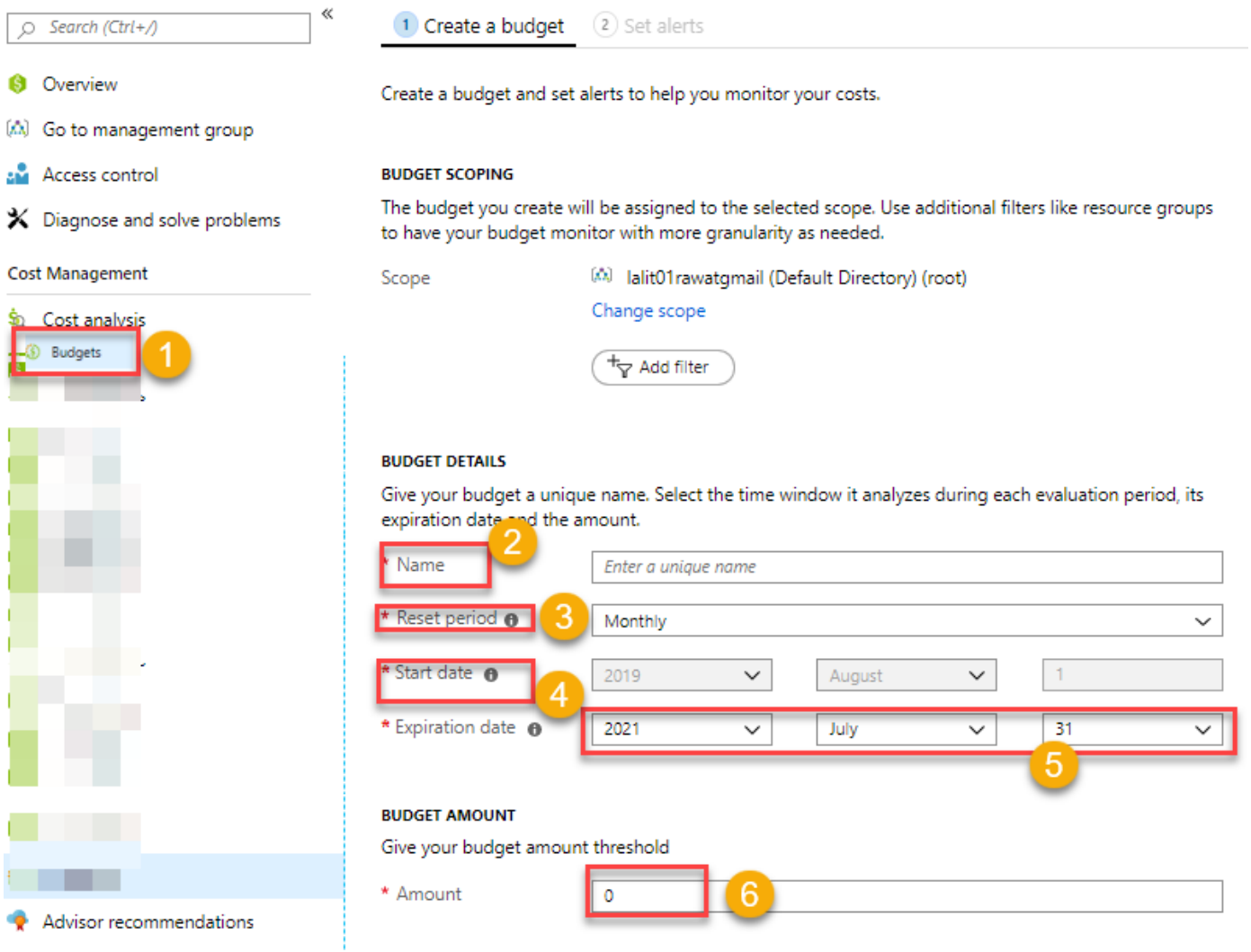
7. Once this is done, click on the Next button to create the alert.

8. Click on Alert conditions and set the alert % number based on your budget. Let's say your total budget is 5K. Once you have spent up to 60% (3000 $), you will get an alert. You can change this setting as well.

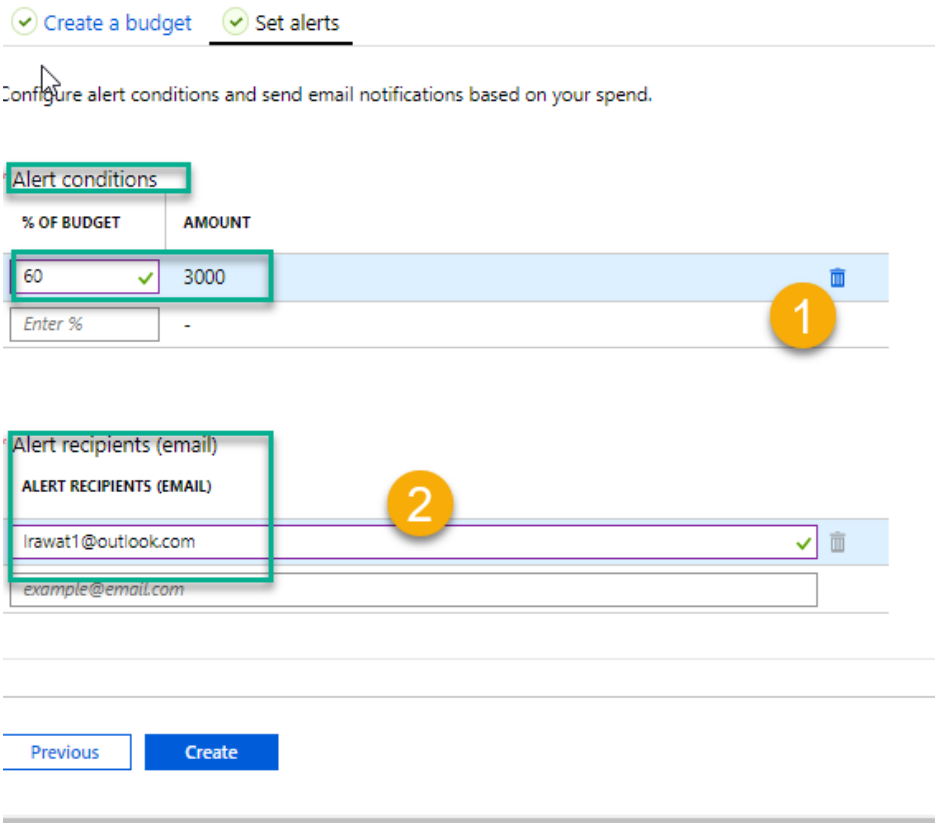
9. Provide the email ID of your users or IT team to get the budget alert.

10. Click on Create and your alert will be created soon.

11. Perform the following steps as shown in the following screenshot:



12. Add the conditions as shown in the following screenshot:



5- Azure subscription policy

The Azure subscription policy or Azure policy is used to achieve the compliance of your organization. It helps you to control the Azure environments as per your organization's compliance prospects.

You can create, manage, modify, and assign the policy based on your organization standards. It will also help you to identify the non-compliance resources in your subscription.

Let's take an example that your organization needs to deploy a specific VM (Virtual Machine) instance size (VM size) in your subscription, and you want to disallow the rest of them, then you can achieve this using the subscription policy.

The second example would be if your company resides in Asia or the US region with few states:

- If you want to allow access, users can create the resources in the specific region and then you can choose the allow location policy and allow only specific locations.
- All the other locations can be denied automatically.

The *allow location policy* will help health care, financial, government services, and so on to achieve compliance specific to the location.

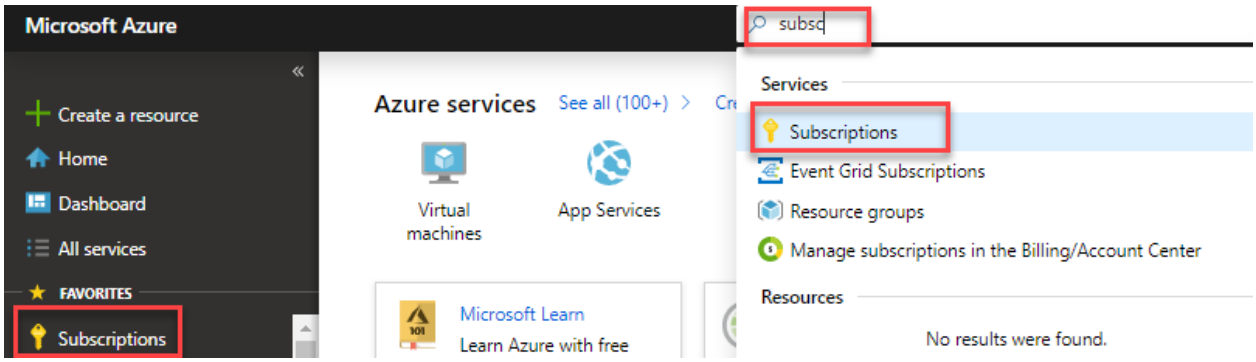
5.1- Azure policy creation, configuration, and assignment

In this section, we will learn how to implement, manage, and implement the policy. For the Azure policy configuration, follow these steps:

1. Login to Azure portal (https://portal.Azure.com).

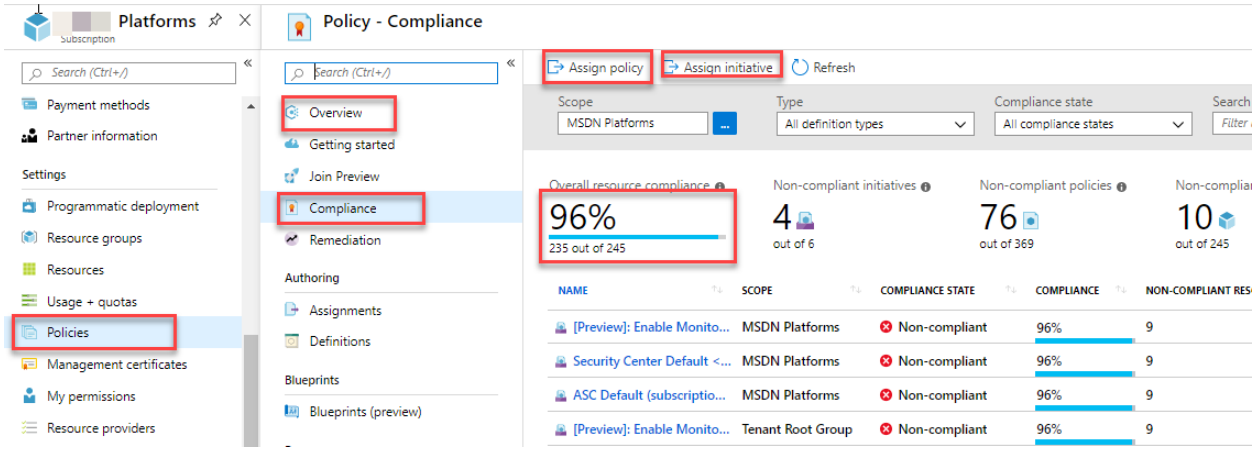
2. Click on search or on the left-hand side of the page in the FAVORITES section. Then, select the Subscriptions option.

3. In the Subscriptions section, click on the settings and select policies and follow the steps as shown in the following screenshot:



4. When you click on the Policies, you will be able to see the assigned policy in your subscription.

5. As you can see, I have applied a couple of policies in the subscription, and you can see the compliance level of the subscription. Follow the steps as shown in the following screenshot:

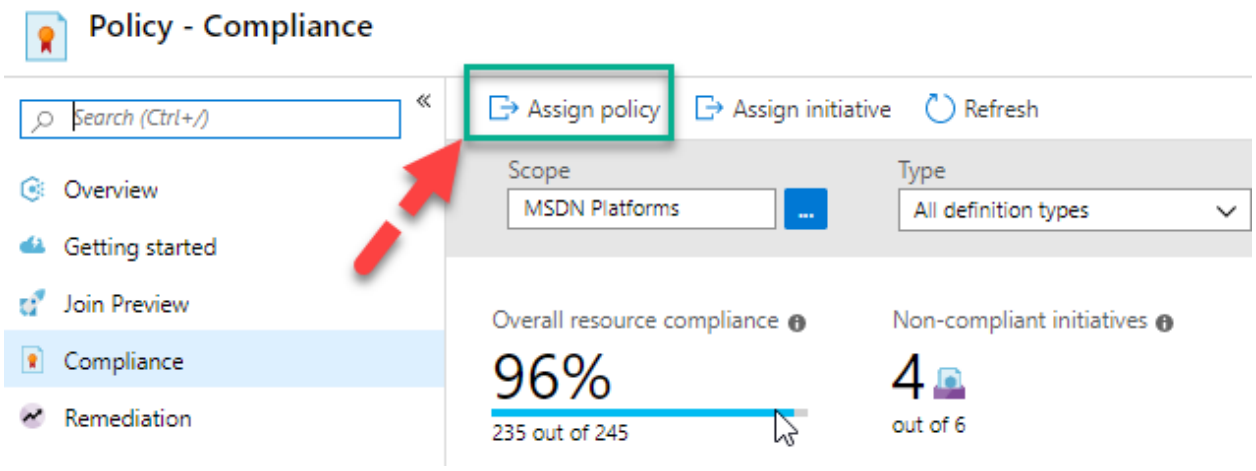


6. If you want to create the new policy, click on Assigned policy.

7. It redirects you to a new screen, and here we can create a new policy.

8. You can provide the following values in your Azure policy. The policy will be created for a specific region:

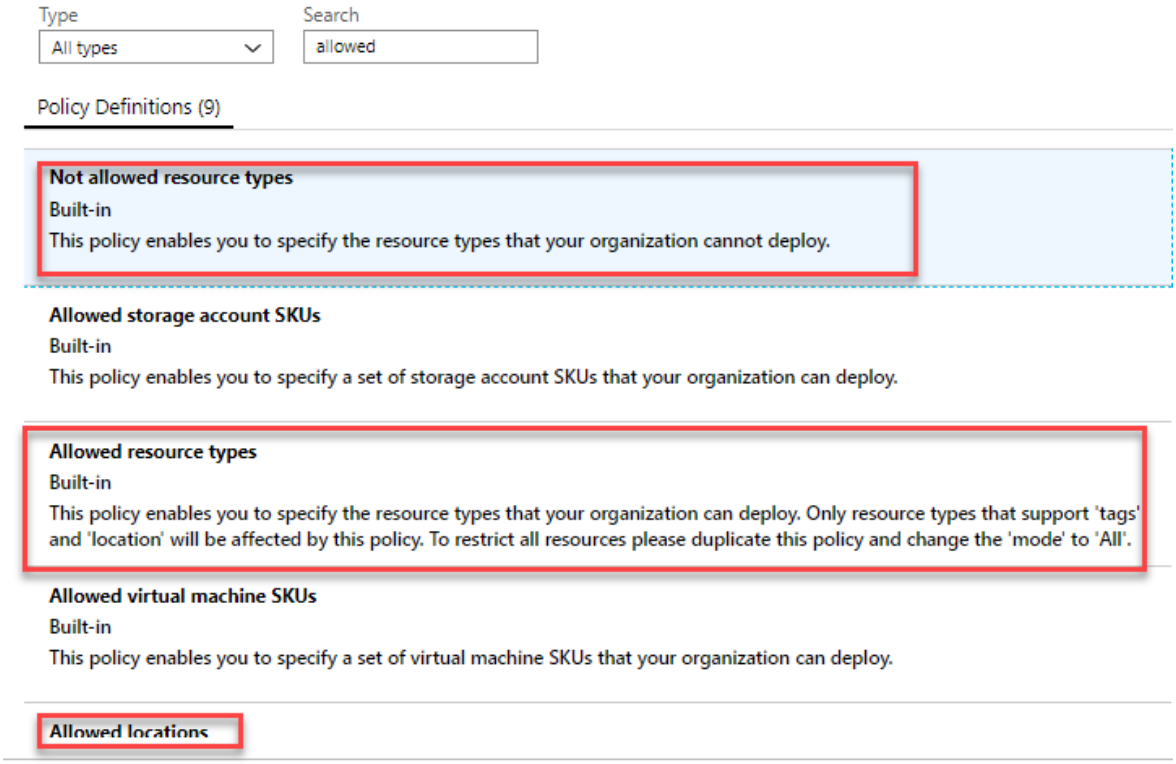
Scope: Provide the subscription as shown in the following screenshot:



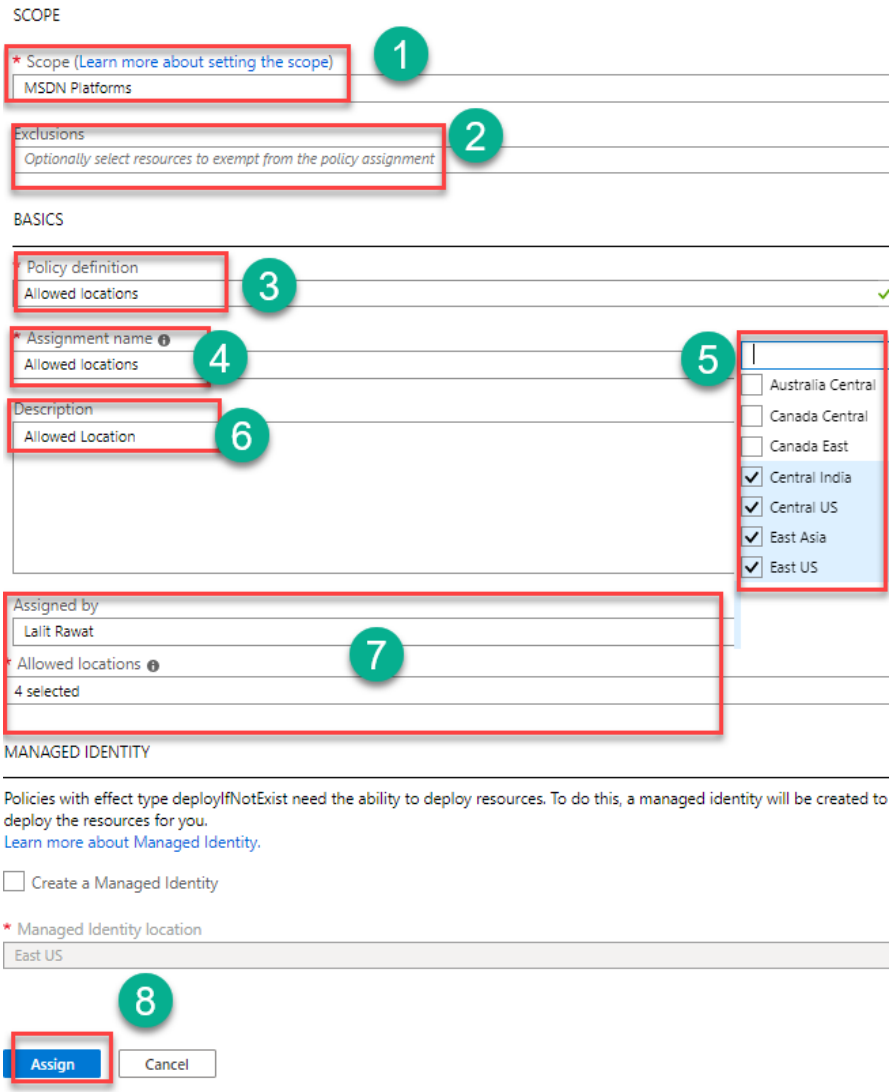
- **Exclusions:** This option can be used if you want to exclude the resources from the policy. If you want to apply to the entire subscription, then do not select any resources in the exclusion policy.

- **Policy definition:** Policy definition will help you to choose the defined policy from the policy gallery to control your resources.

Follow the steps as shown in the following screenshot:



- If you are planning to have the resources in a specific location, then click on the Allowed locations policy.
- If you want to allow a specific SKU, then you can achieve this by using the Azure policy.
- Take a look at the following specific policy. You can search and apply the policy based on your organization's standard policy. Refer to the following screenshot:



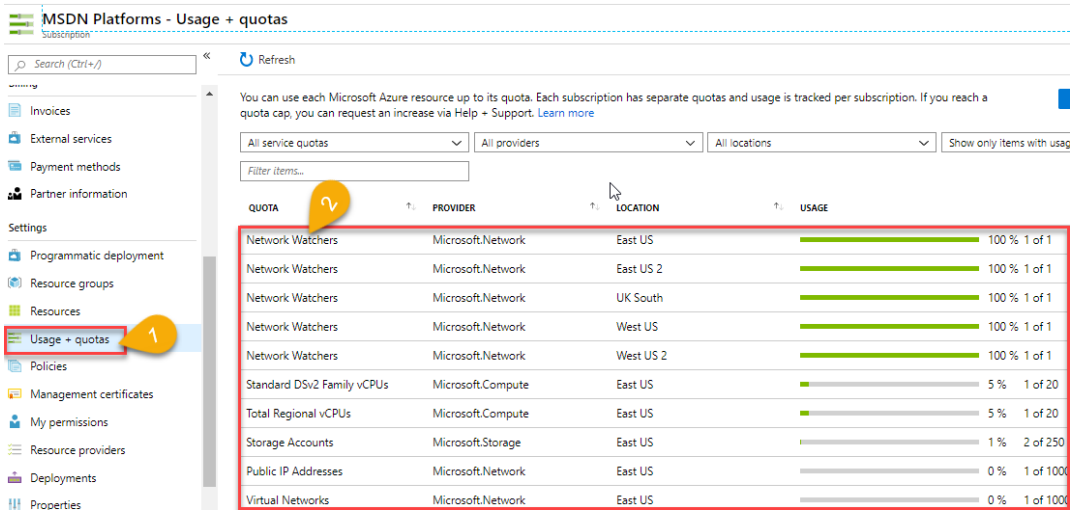
6- Azure quota

An Azure quota is nothing but the limitation of a specific subscription of how many resources can be deployed. Generally, a quota is of two types:

- **Soft limit:** Default resources available in the subscription can be increased by raising the request with the MS team.
- **Hard limit:** Maximum resources can be deployed within the subscription and even raising the request with the MS team cannot be increased.

If you want to see the usage limit and quota of your subscription, then click on the subscription. In the Settings section, click on Usage + quotas, and you will be able to view the available services in your subscription and see the quota as well.

You can see the details of the subscription limitation in the following screenshot:



7- Resource tag

We can use the Azure resource tag to add the extra fields to identify the resources and it can be used for billing purposes. Every tag contains the following fields:

- **Name: Production Application**
- **Owner: Lalit Rawat**
- **Department: IT**
- **Bill to: IT**

Note: The preceding resource tags are just examples that can be changed based on your organization's policy. Based on that, you can define the tags and associate specific resources.

7.1- Usage of the resource tag

Let us say if you are a big organization and have deployed 4,000 applications, then how can you understand which resources group belongs to which app and who is the owner? Who to bill the usage of services which is presented in the resources group?

Hence, to identify the billing purpose, resource group tags can be used, and they are very helpful in the long term for a structured organization. Perform the following steps:

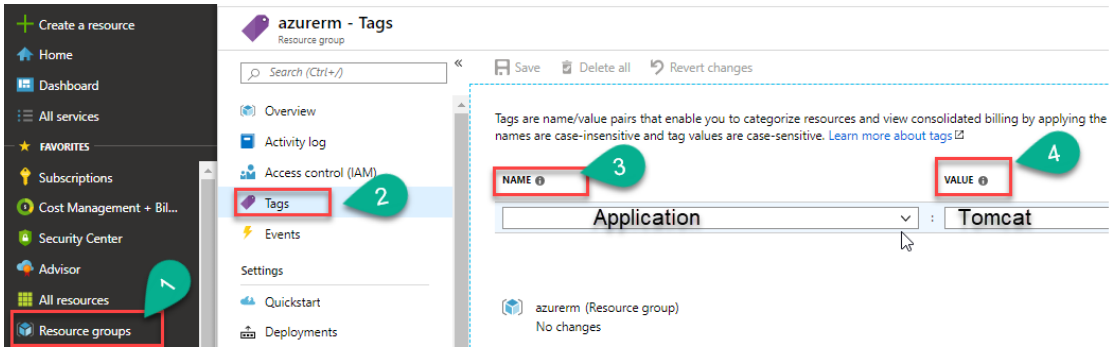
1. Click on **Resource groups**.

2. Under the **Overview** tab, click on the **Tags** option.

3. Provide the resource name, application, owner, database, and so on.

4. Then, provide the values, where values is your application name like Tomcat, Apache, SQLDB, and so on.

5. Click on **Save** as shown in the following screenshot:



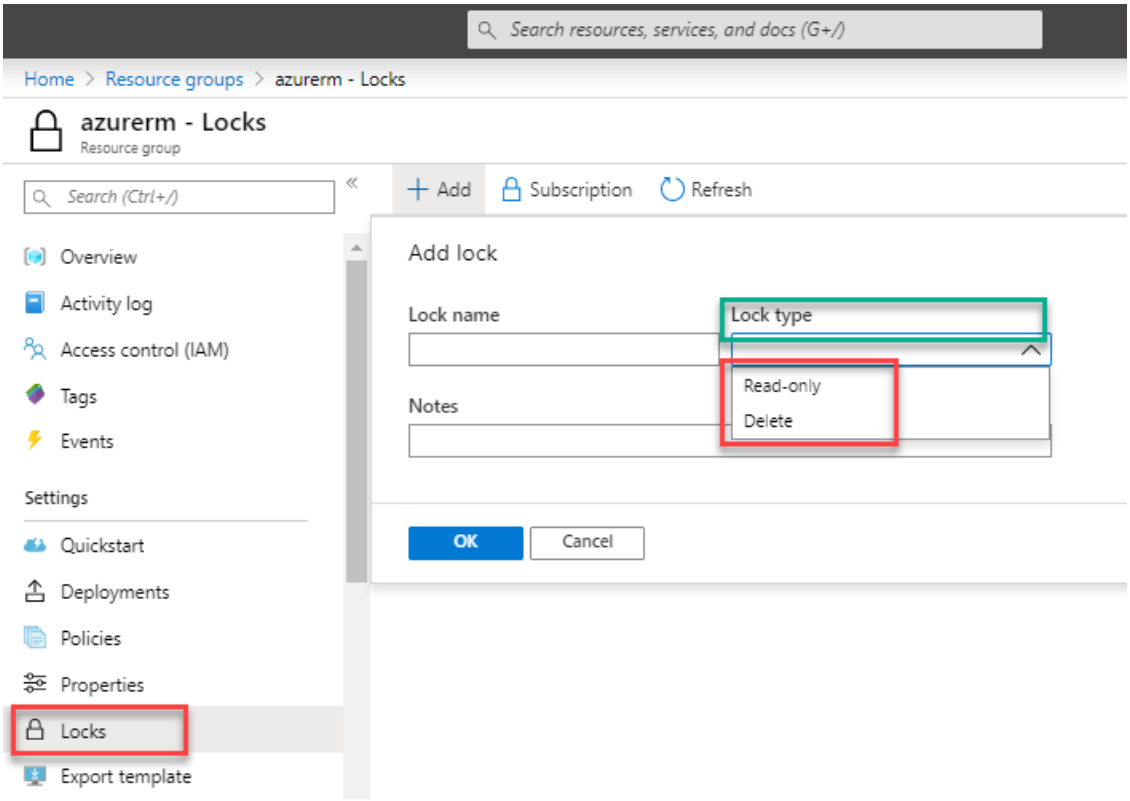
7.2- Configuration of a resource lock

The resource lock will help you with your accidental deletion of resources.

Administrators can lock the resources to prevent others from deleting the resources.

In the subscription, you can find two types of locks:

- **Delete:** This lock prevents resources from users deleting the resource. However, users can still read and modify the resource.
- **Read-only:** This lock provides access to read-only resources; in that case, users cannot modify or change the resources. However, they can still see the resources.



If you want to apply a lock on your resource group, follow the given steps.

1. Log in to the Azure portal by opening https://portal.Azure.com .

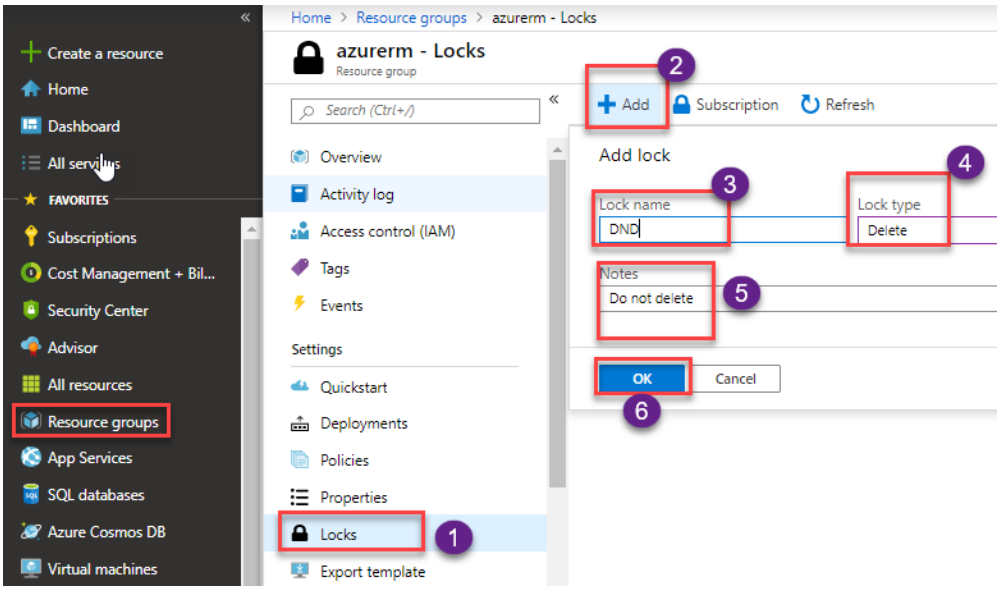
2. Select Resource groups.

3. Under the resources group, click on Locks.

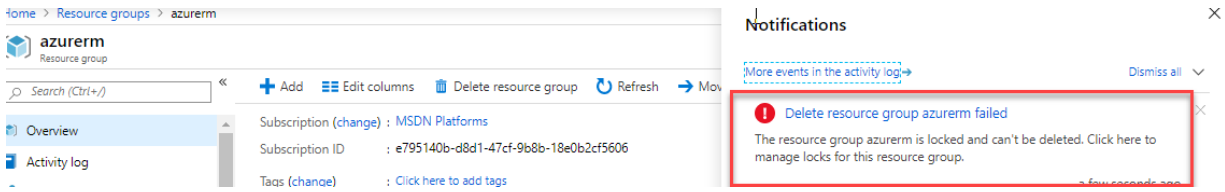
4. Create a lock.

5. After the lock creation, you can deploy the lock-in resource group successfully.

6. Perform the following steps as shown in the following screenshot:



7. If you try to delete the resources, you will get the message that the resources group has been locked and cannot be deleted as shown in the following screenshot:



7.3- Resources movement from one resource group to another

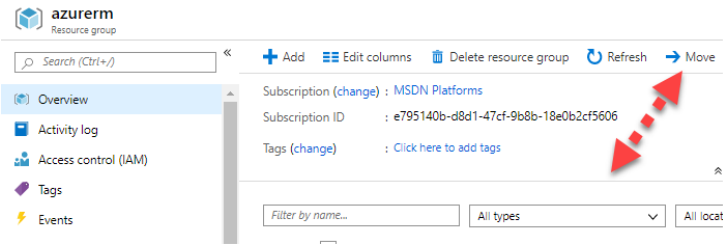
If you are planning to move the resource group resource (VMs and so on) to another resource group, then this can be done easily.

You can also migrate the resources between subscriptions under the same tenant, and this can be done using the portal.

If you want to move the resources, perform the following steps:

1. Click on the resources group in which you want to move the resources.

2. Select the Move button at the top-right corner of the screen as shown in the following screenshot:

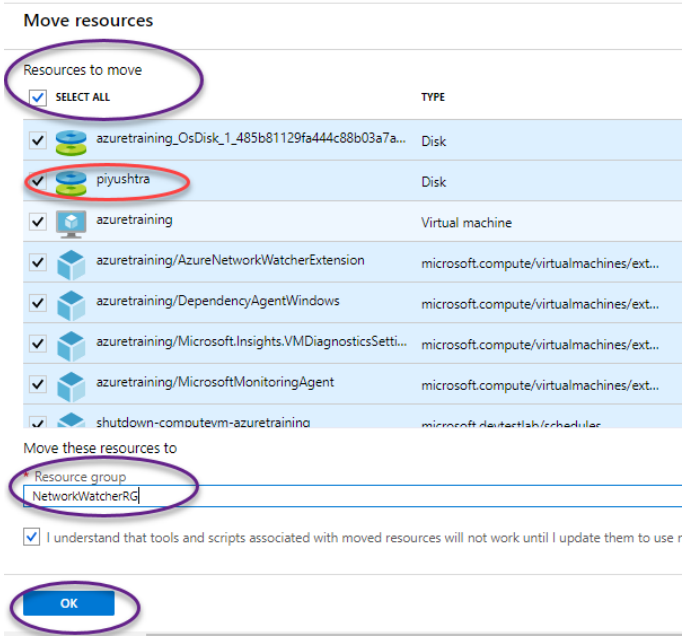


3. Select the resources you want to move from one resource group to another.

4. Click on OK.

5. It will take 45 to 20 minutes based on the size of the resource to complete the task.

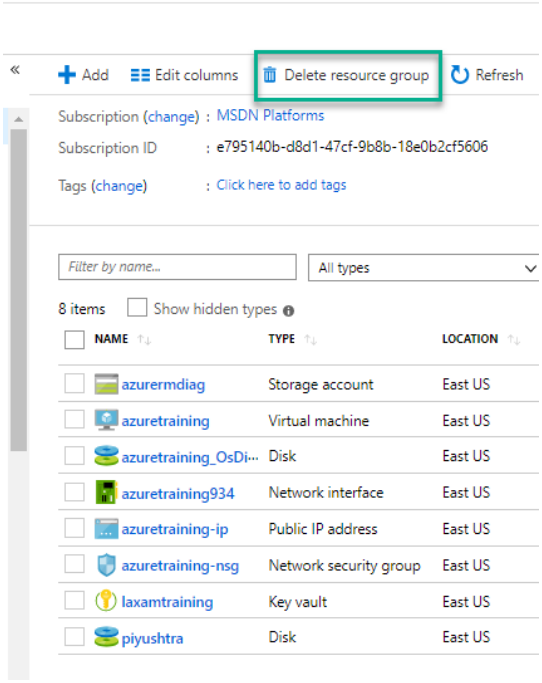
6. Follow the given steps as shown in the following screenshot and click on Move to move to the new resources group.



7. When you click on your resources, the resources will be migrated to a new resources group.

7.4- Removing a resource group

A resource group can be removed by clicking on the delete resource group. This can be done through the Azure portal, CLI, PowerShell, and so on. Take a look at the following screenshot:



Perform the following steps:

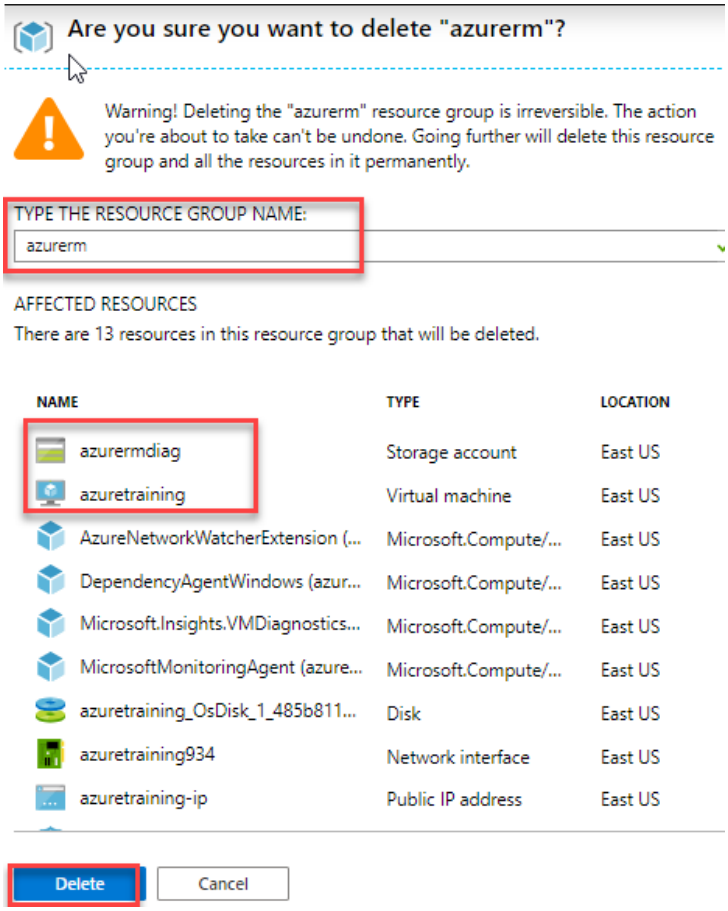
1. Click on the delete resources group.

2. Provide the resource group name.

3. Once you provide the resources group name, click on the Delete button.

4. Once done, the resources will be deleted automatically.

Take a look at the following screenshot for more details:



8- Creating and configuring the management groups

The management group will help you to manage multiple subscriptions in a single tenant. We can efficiently manage the access, policies, and compliance for these subscriptions.

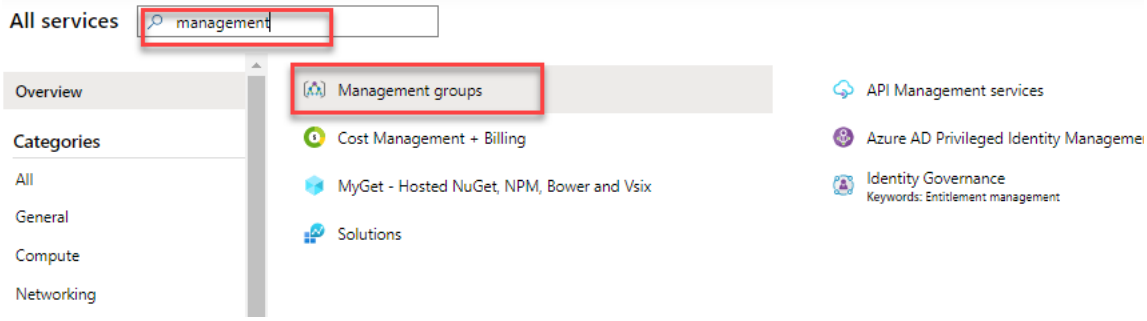
We can apply the single policy within the tenant group. The first management group will act as a tenant, and the policy that applies on this subscription will be inherited to other subscriptions as well.

If you want to create and configure the management group, follow the given steps:

1. Click on all services.

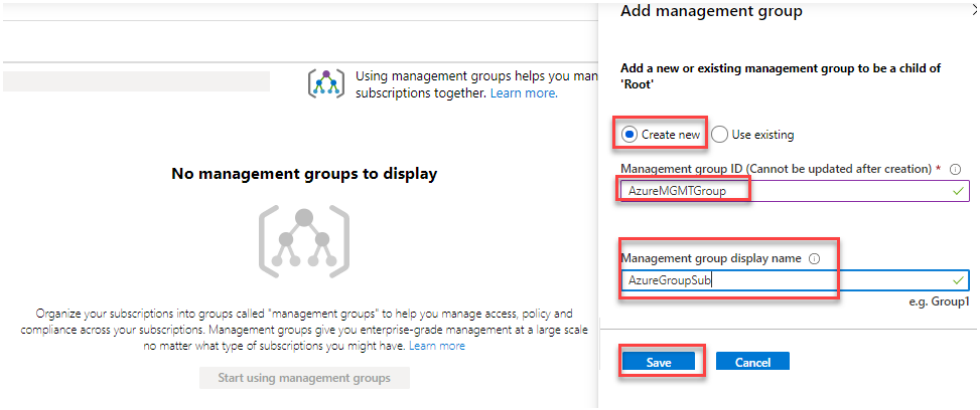
2. Type *management* in the search box.

3. Click on the **Management groups** option, as shown in the following screenshot:

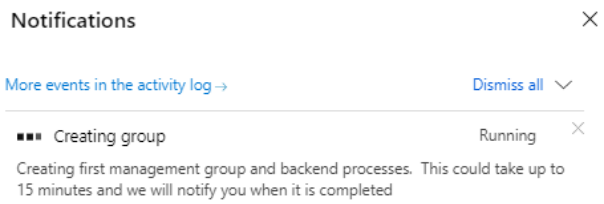


4. Once you click on the management group:

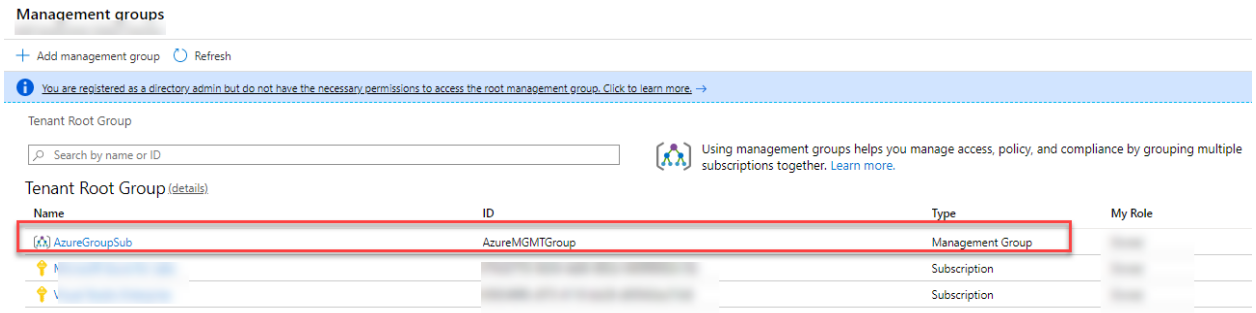
- Click on **Create new**.
- In **Management group ID (Cannot be updated after creation)***, provide the name.
- Provide the management group display name.
- Click on **Save** as shown in the following screenshot



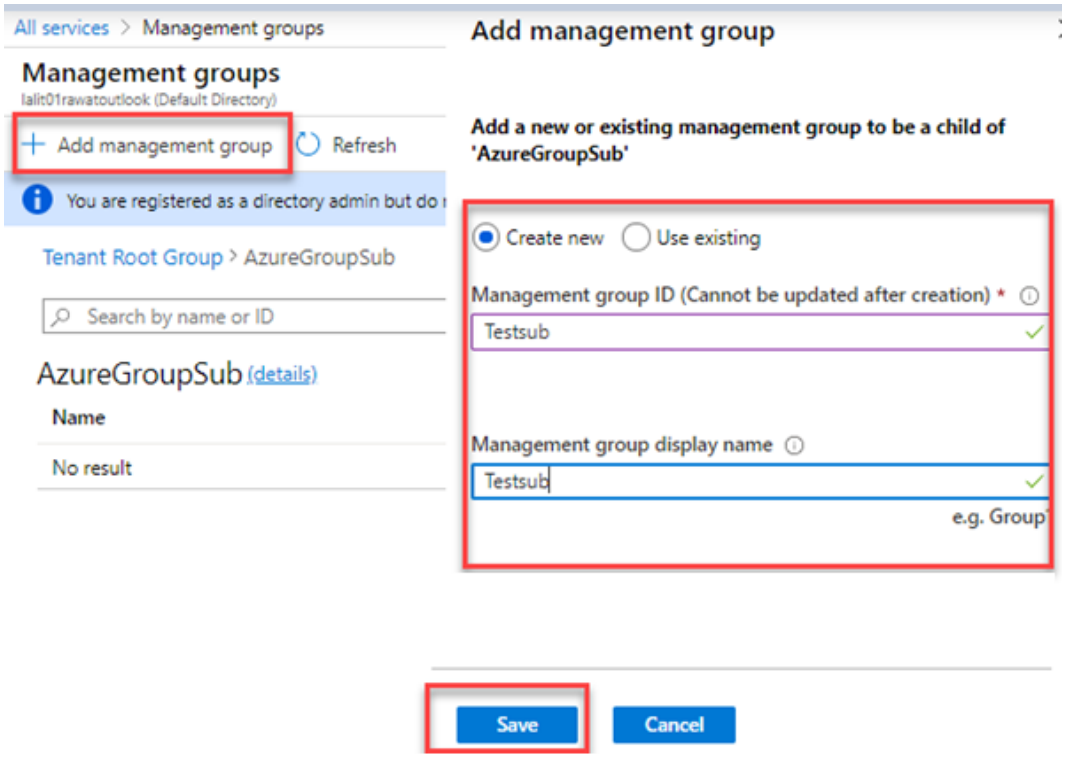
5. Once you click on Save, it will start creating the first management group which might take up to 15 minutes. Refer to the following screenshot:



6. Once the management group is created, you will see the following screen as shown in the following screenshot:



7. If you want to create another management group, then click on the + Add management group and create another group as shown in the following screenshot:



8. Once the management group is created, you need to assign the subscription to the management group so that when you apply the policy, it

should be inherited to the subscription associated with the management group. You can configure it as shown in the following screenshot:

9. Now, we will complete this step to configure the management group and associate it with the subscription: