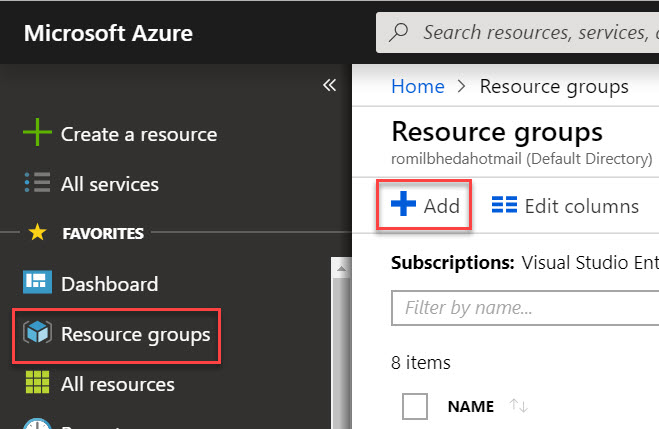
**Azure Resource Group**

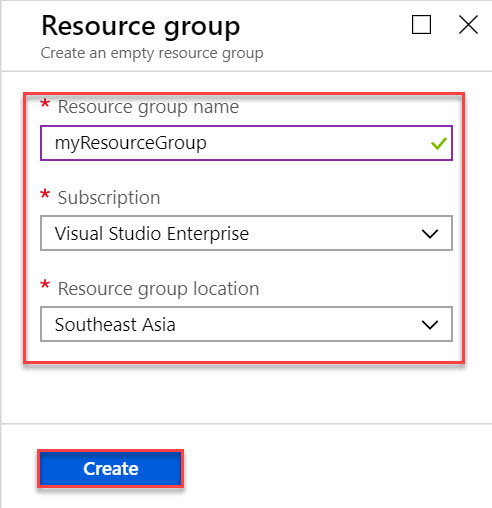
**Step 1:** Open Microsoft Azure Portal and enter credentials

<https://portal.azure.com>

**Step 2:** Click on **Resource Groups ->** Click on **+ Add**



**Step 3:** Create New Resource Group

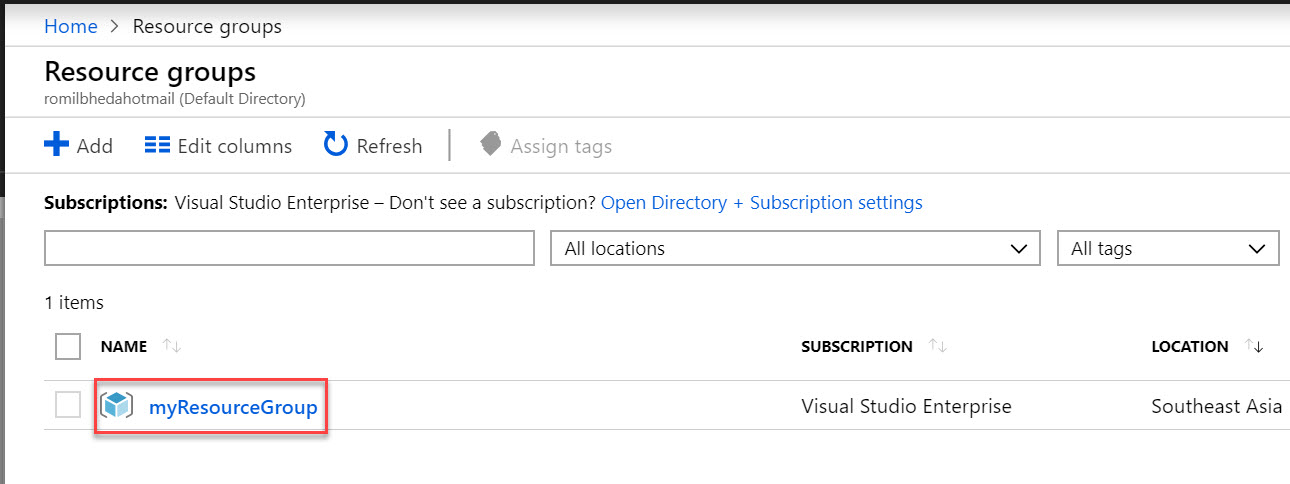


**Resource Group Name:** myResourceGroup

**Subscription:** Choose any working

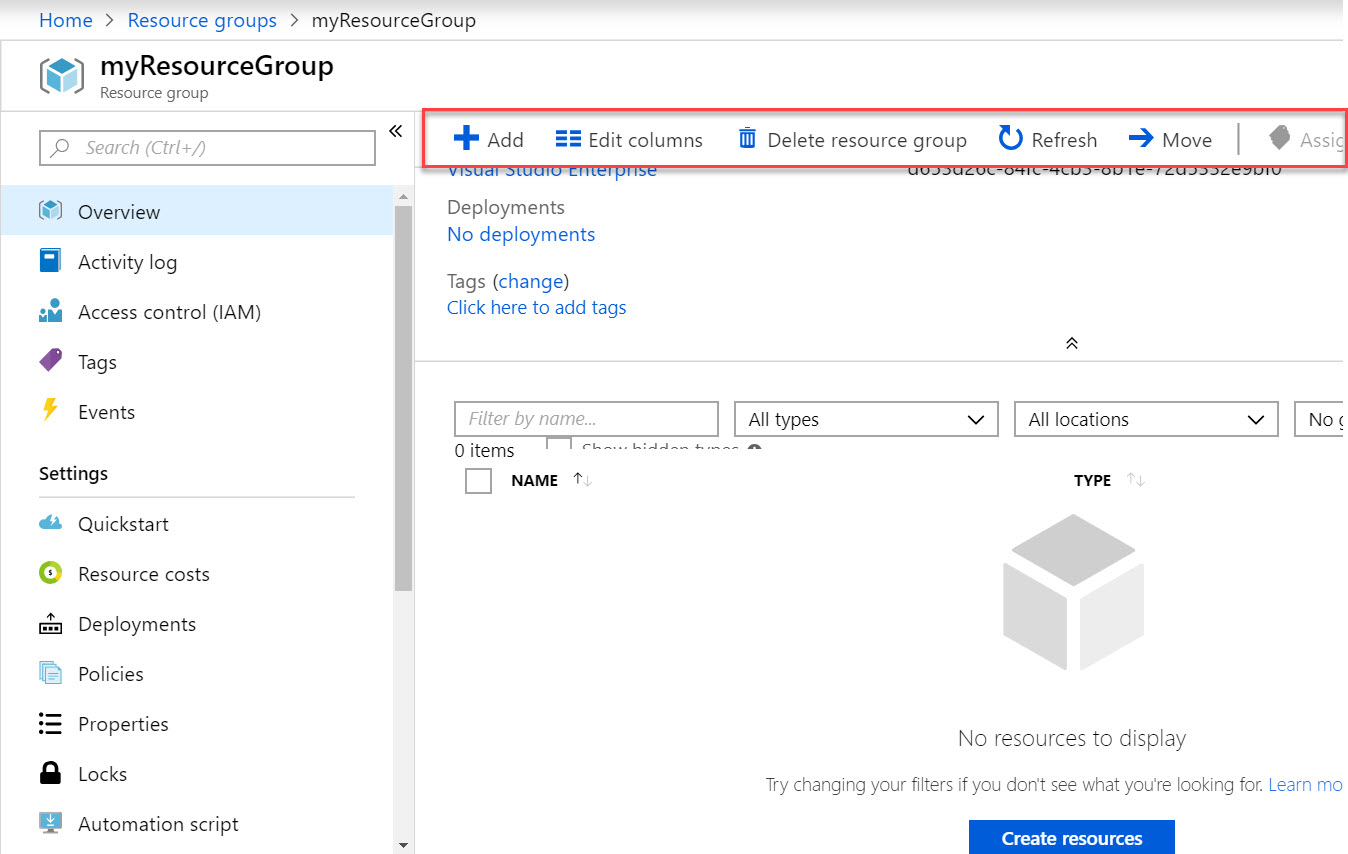
**Resource group location:** nearest region

**Step 4:** All Resource Group will list here:



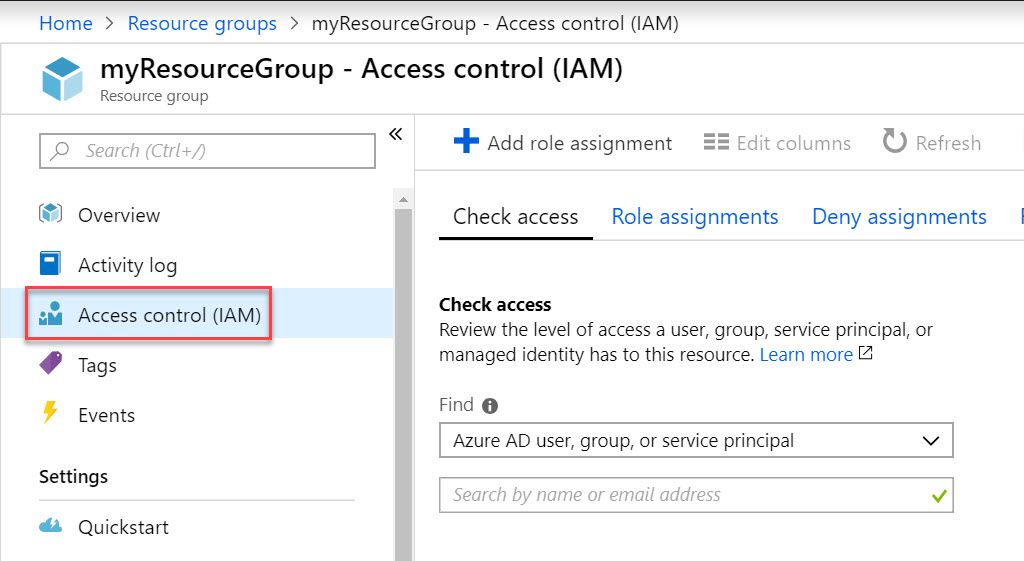
**Step 5:** Add new resource under same resource group please click on **+ Add**

Other operations also available: Edit columns, Delete Resource Group, Refresh, Move, Assign Tags

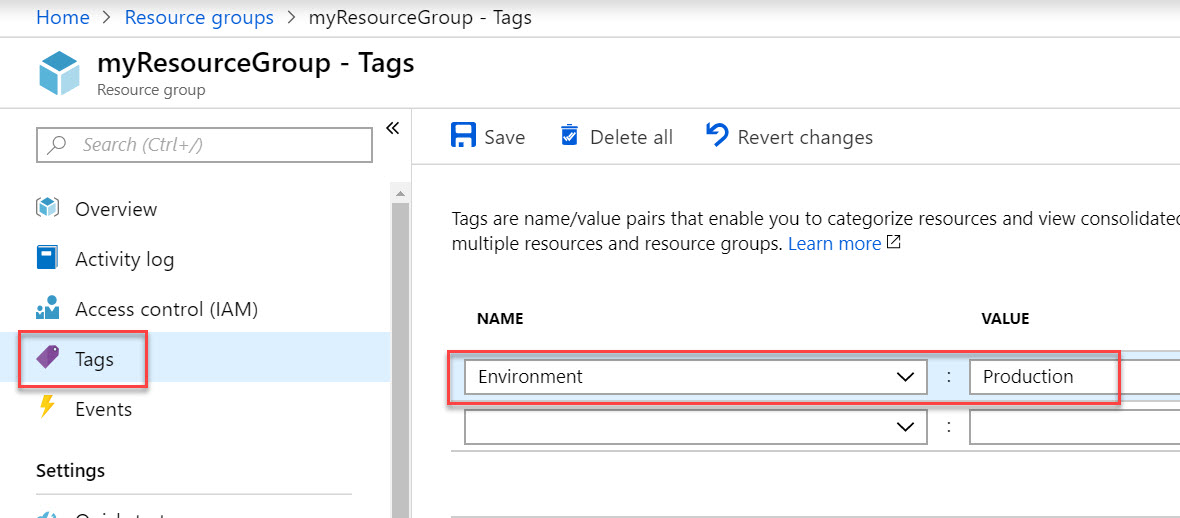


**Step 6:** **Access Control (IAM)** also known as identity and access management.

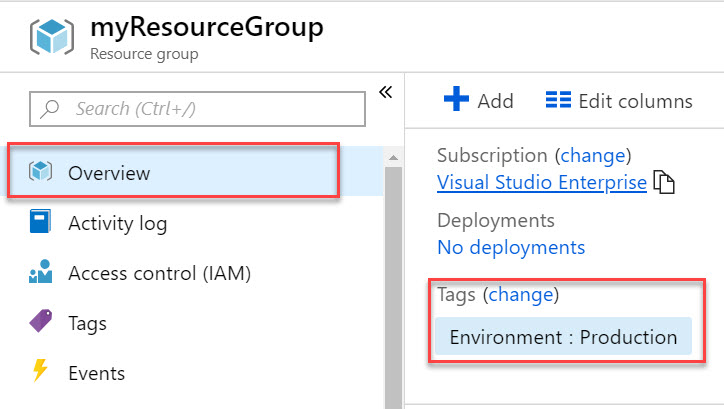
With this option you can perform role assignment and permissions also known as Role-Based Access Control (RBAC). You can share or assign role to this resource group with other members and so on.



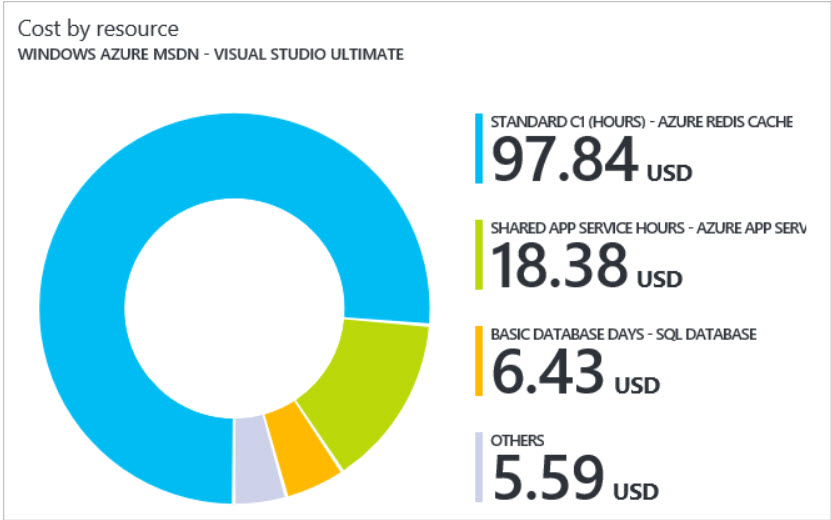
**Step 7:** **Tag** -> You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy. Each tag consists of a name and a value pair. For example, you can apply the name "Environment" and the value "Production" to all the resources in production.



Under Overview option you can find Tags. Ex. Environment: Production

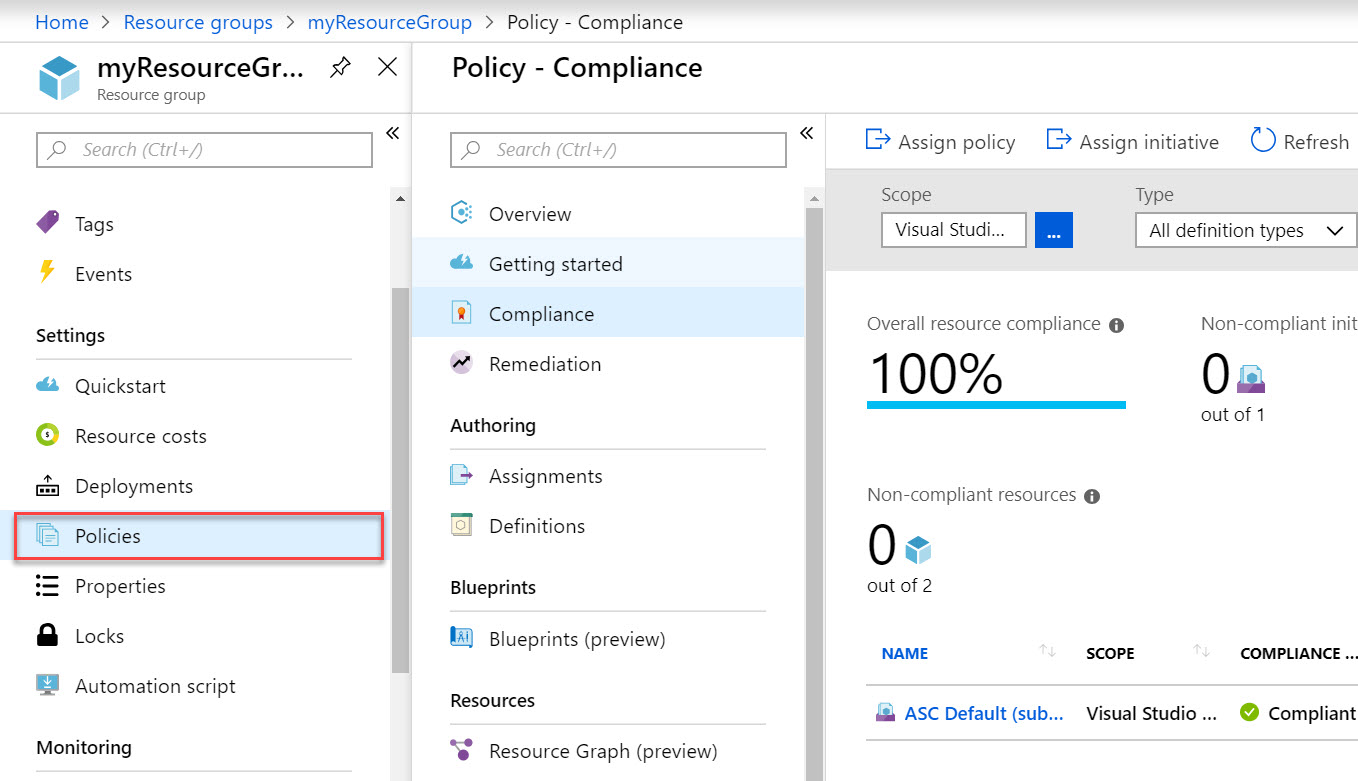


**Step 8:** Can check Resource wise costing



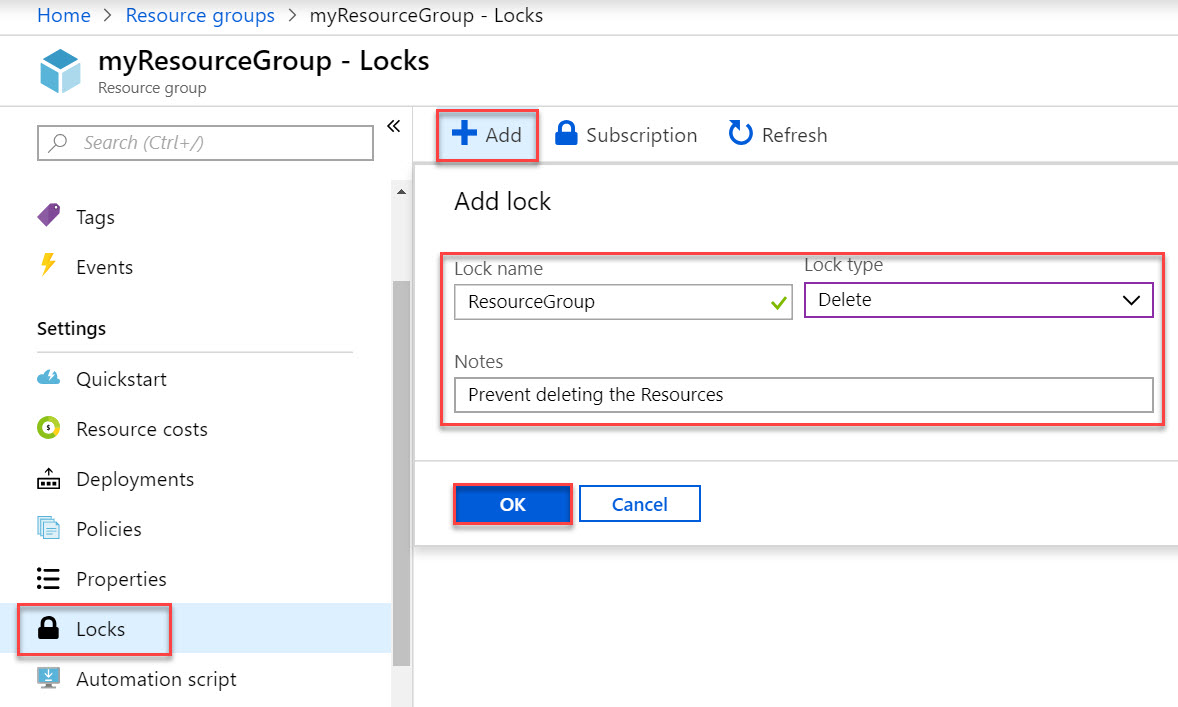
**Step 9: Policies**

Azure Policy is a service in Azure that you use to create, assign and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies. For example, you can have a policy to allow only a certain SKU size, location, type of virtual machines or any other services in your environment.



**Step 10:** **Locks**

As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to **CanNotDelete** or **ReadOnly**.



**Step 11:** **Monitoring** -> Modern applications are often complex and highly distributed with many discrete parts working together to deliver a service. Recognizing this complexity, Azure Monitor provides monitoring insights for resource groups.



**Step 12:** **Delete Resource Group**

Deleting a resource group deletes all the resources contained within it. You can also delete individual resources within a resource group. Use caution when deleting a resource group. That resource group might contain resources that resources in other resource groups depend on.

