***Azure Resource Groups Overview:***

An Azure Resource Group is a logical container that holds related resources for an Azure solution. It allows you to group resources (such as virtual machines, storage accounts, databases, etc.) together so that they can be managed and organized more easily. Resource groups provide the following benefits:

**Resource Management:** You can manage all resources in a group as a unit, like deploying, updating, or deleting them together.

**Access Control:** Apply Role-Based Access Control (RBAC) at the resource group level, controlling who can perform actions on the resources within it.

**Cost Management:** Monitor the cost and usage of all resources in the group.

**Scoping Policies:** Azure policies can be scoped to a resource group to enforce compliance across all resources within the group.

**Key Concepts:**

1. **Resource Group Creation:**

When you create a resource in Azure, you must specify a resource group to associate it with.

Resources within the same group can be managed together, but they can also have different locations.

1. **Organizing Resources:**

Best practices suggest grouping resources that share the same lifecycle (e.g., all resources related to a particular application).

You can also group resources based on their environment (production, testing, development) to easily manage and enforce security rules.

1. **Scoping Policies and Permissions:**

**Azure Policies:** You can enforce rules and standards at the resource group level (e.g., restricting the creation of VMs in certain regions).

**RBAC:** Control access to all resources in the group by assigning roles to users, groups, or applications at the resource group level.

***Practical Task: Create and Manage Azure Resource Group:***

**Step 1: Create a Resource Group**

1. In the **Azure Portal**, search for **Resource Groups**.
2. Click **Create**.
3. Provide a **Resource Group Name** (e.g., "FinancialApp-RG").
4. Select a **Region** (e.g., "East US").
5. Click **Review + Create**, then click **Create**.

**Step 2: Add Resources to the Resource Group**

1. Once the resource group is created, open it.
2. In the resource group, click **Add**.
3. Choose a resource to deploy (e.g., Virtual Machine, Storage Account).
   * For a VM, you can deploy Ubuntu, Windows, etc.
   * For storage, choose **Storage Account** and provide the necessary details.
4. After deployment, verify that the resources are added to the resource group.

**Step 3: Apply Access Controls (RBAC)**

1. Open the resource group and go to **Access Control (IAM)**.
2. Click **Add role assignment**.
3. Select a **Role** (e.g., "Contributor"), then assign it to a user (e.g., "Lokesh").
4. Click **Save**.
   * Now, Lokesh has access to all resources within this resource group based on the assigned role.

**Step 4: Apply Policies at the Resource Group Level**

1. In the resource group, click on **Policies**.
2. Click **Assign Policy**.
3. Choose a policy definition (e.g., "Allowed Locations") to restrict the locations where resources can be deployed.
4. Set the scope to your resource group and enforce compliance.

***Time-based access control***

Time-based access control in Azure allows you to grant users or groups access to resources for a specified period. This can be useful for temporary access, like when an employee needs to access a resource for troubleshooting, or a contractor needs short-term access to a project.

You can achieve time-based access control using \*\*Azure Privileged Identity Management (PIM)\*\*, which is part of Azure Active Directory (Azure AD). PIM allows you to manage, control, and monitor access to important resources with just-in-time (JIT) access.

**### Steps to Implement Time-Based Access Control Using Azure PIM**

**1. \*\*Enable PIM for the Subscription or Resource\*\***

1. \*\*Go to Azure Portal\*\*: [portal.azure.com](https://portal.azure.com/).

2. In the left-hand menu, search for \*\*Azure AD Privileged Identity Management\*\*.

3. \*\*Select PIM\*\* and go to the resource (e.g., subscription, resource group) where you want to enable time-based access control.

- For subscription-level access, select \*\*Azure AD roles\*\* or \*\*Azure resources\*\* from the PIM menu.

- You can choose the scope of access control (subscription, resource group, or specific resources).

4. Click \*\*Manage resource roles\*\*.

**2. \*\*Assign a Role with Time Constraints\*\***

1. \*\*Select the Role\*\*:

- Select the role you want to assign (e.g., \*\*Reader\*\*, \*\*Contributor\*\*, \*\*Virtual Machine User Login\*\*, etc.).

- Click \*\*Add assignment\*\*.

2. \*\*Choose the User\*\*:

- In the \*\*Select member(s)\*\* section, select the user or group you want to assign the role to.

3. \*\*Configure Time-based Access\*\*:

- Set the \*\*Activation settings\*\* to enable time-based access.

- Enable \*\*Eligible\*\* assignment (if the user can request elevated access when needed) or \*\*Active\*\* assignment for limited duration.

\*\*Eligible\*\*: User can request elevated access when needed for a specific period.

\*\*Active\*\*: User is granted temporary access for a set duration.

4. \*\*Set Activation Duration\*\*:

- Configure the \*\*maximum activation duration\*\* (e.g., 1 hour, 8 hours, etc.).

- You can also require \*\*justification\*\* for activation and enforce \*\*MFA\*\* (Multi-Factor Authentication) during activation.

5. \*\*Set Start and End Dates\*\*:

- Define the \*\*start\*\* and \*\*end dates\*\* for the time-based access.

- You can schedule the user's access to be automatically activated and revoked within the defined time period.

6. \*\*Save the Assignment\*\*.

**3. \*\*Access Review (Optional)\*\***

- To periodically review who has access, you can set up \*\*Access Reviews\*\* within PIM to ensure users still need access to specific resources.

- Access reviews can be configured to alert admins when access is no longer needed or has expired.

**Example Scenario for Time-Based Access**

- You have a \*\*contractor\*\* (e.g., `contractor@company.com`) who needs access to a \*\*frontend VM\*\* only for the next 3 days to perform some maintenance.

**\*\*Steps\*\*:**

- Assign the \*\*Virtual Machine User Login\*\* role to the contractor for the \*\*Frontend VM\*\*.

- Set the access as \*\*Eligible\*\* with a duration of 8 hours per activation.

- Set the start and end date to limit access to 3 days.

- Require \*\*MFA\*\* and a \*\*justification\*\* to elevate their access.

The contractor will have access only during the specified time window and can elevate their privileges to perform tasks for 8 hours at a time (subject to your configuration).

***Benefits of Time-Based Access Control***

1. \*\*Improved Security\*\*: Users only have access when needed, reducing the risk of unnecessary access over time.

2. \*\*Reduced Attack Surface\*\*: Temporary access reduces the chances of long-term misuse of privileged roles.

3. \*\*Auditing\*\*: All role activations and time-based access changes are logged, providing a clear audit trail.

***Locks:-***

Azure \*\*resource locks\*\* allow you to protect critical resources from accidental changes or deletions. Resource locks can be applied to \*\*subscriptions\*\*, \*\*resource groups\*\*, or individual \*\*resources\*\* (like a virtual machine). Locks come in two types:

1. \*\***Read-only\*\*:** Only viewing the resource is allowed, but no actions can be performed on it.

2. \*\***Delete**\*\*: The resource can be modified, but it cannot be deleted.

**0.Steps to Lock a Virtual Machine in Azure**

**1. \*\*Lock the Virtual Machine\*\***

1. Go to the Azure portal

2. Navigate to the \*\*Virtual Machines\*\* section and select the VM you want to lock.

3. On the \*\*VM overview page\*\*, scroll down to \*\*Settings\*\* in the left-hand menu and select \*\*Locks\*\*.

4. Click \*\*Add\*\* to create a new lock.

5. In the \*\*Add lock\*\* pane:

- \*\*Lock Name\*\*: Enter a name for the lock (e.g., `LockVM`).

- \*\*Lock Type\*\*: Choose one of the following:

- \*\*Read-only\*\*: This will prevent any changes (updates, stops/starts, etc.) to the VM. Only read access is allowed.

- \*\*Delete\*\*: This will allow changes but prevent the VM from being deleted.

6. Click \*\*OK\*\* to apply the lock.

**2. \*\*Verify the Lock is Working\*\***

Once the lock is applied, you can try to verify that it is working:

**For a \*\*Read-only\*\* lock:**

1. Try performing an action on the VM, like starting or stopping it.

- Navigate to the VM's \*\*Overview\*\* page.

- Try to \*\*Start\*\*, \*\*Stop\*\*, or \*\*Restart\*\* the VM.

- Azure should show an error message indicating that the resource is \*\*locked\*\* for editing.

\*\*Expected Result\*\*: You should see an error indicating that the action is not allowed because the VM is locked.

**For a \*\*Delete\*\* lock:**

1. Try deleting the VM.

- On the \*\*Overview\*\* page of the VM, click \*\*Delete\*\*.

- Azure should display an error preventing the deletion.

\*\*Expected Result\*\*: An error message should appear, stating that the VM cannot be deleted because it has a \*\*delete lock\*\*.

**1. Locking a Resource Group**

* If you lock a resource group (either with a **Read-only** or **Delete** lock), all resources within that group will inherit the lock.

**Read-only Lock**:

* + You cannot modify or change any resource inside the group. This includes virtual machines (VMs), databases, networks, etc.
  + Actions like starting/stopping VMs, scaling, or changing configurations are not allowed.
  + You can only **view** the resources.

**Delete Lock**:

* + Resources inside the resource group can still be **modified** (e.g., you can start/stop a VM or change settings), but **deletion** of any resource or the resource group itself is not allowed.
  + You cannot delete the resource group or any individual resources within it.

**2. Locking a Subscription**

* If you lock a subscription, the lock applies to **all resource groups and resources** within that subscription.

**Read-only Lock**:

* + You cannot perform any changes across any resource within the subscription, including virtual machines, databases, and any other services.
  + You can only **view** the subscription and its resources.

**Delete Lock**:

* + Resources in the subscription can be modified, but **no resource or resource group can be deleted**.
  + You cannot delete the subscription itself or any individual resources under it.

**Use Case for Locks:**

- \*\*Read-only Lock\*\*: Prevent users from accidentally starting or stopping a production VM.

- \*\*Delete Lock\*\*: Prevent accidental deletion of critical VMs or any resources that shouldn't be easily deleted.

***Service principle creation:-***

To manage Azure resources like storage accounts, VMs, or others using automation tools or non-user-based access, you often use a **Service Principal**. A service principal allows your application, script, or automation tool to authenticate and access Azure resources securely without human intervention. Here's how you create a service principal, assign a role, and use it to access resources like VMs or storage accounts.

**Example:=**

You are developing an application that needs to programmatically upload files to an Azure Storage Account.

Instead of giving this application access to your Azure account credentials, you create a **Service Principal** that the application can use to securely interact with the storage account.

The application will use the **Storage Blob Data Contributor** role to upload and manage blobs.