ASSIGNMENT

DevOps Pro

SUNBMITTED BY

MANISH KUMAR
mmaurya694@gmail.com

UNDER THE GUIDANCE OF

Hitesh Choudhary & Saksham Choudhary

Assignment Part-4

Question 1. What is the need of IAM?

Ans. It helps protect against compromised user credentials and easily cracked passwords that are common network entry points for criminal hackers who want to plant ransomware or steal data.

Done well, IAM helps ensure business productivity and frictionless functioning of digital systems.

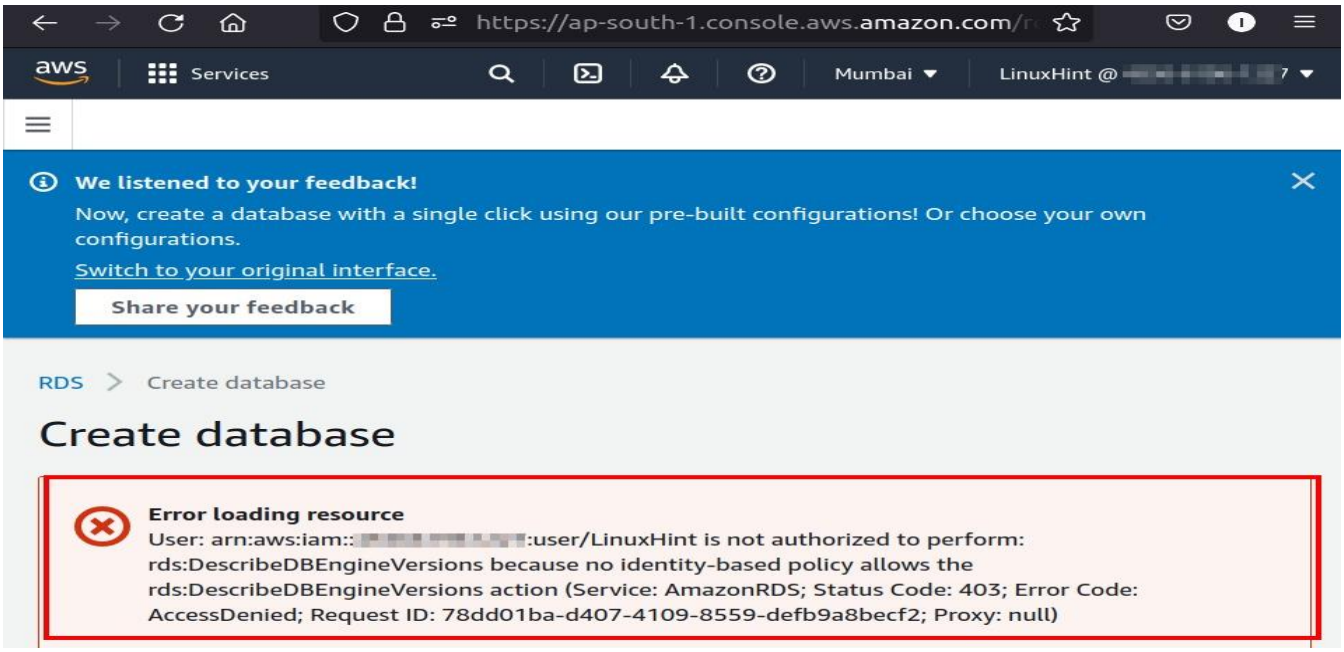
Question 2. If i am a non tech person, how will you define policies in IAM.

Answer. IAM is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources. An AWS IAM policy defines the permissions of an identity (users, groups, and roles) or resource within the AWS account. An AWS IAM policy regulates access to AWS resources to help ensure that only authorized users have access to specific digital assets. Permissions defined within a policy either allow or deny access for the user to perform an action on a specific resource.

IAM policies can either be identity-based or resource-based. Identity-based policies are attached to an identity (a user, group, or role) and dictate the permissions of that specific identity. In contrast, a resource-based policy defines the permissions around the specific resource—by specifying which identities have access to a specific resource and when. Identity-based policies and resource-based policies both uphold IAM security standards and give organizations flexibility with how to best set up their resource management strategy to meet their needs.

Question 3. Please define a scenario in which you would like to create your on own IAM policy.

Ans. we have created an IAM user who, by default, cannot create or modify RDS resources due to permission barriers. For e.g., in its current state, without any policy attached, this IAM user cannot create an RDS DB instance. If we try to create an RDS DB from the RDS console of this IAM user, we get the following error

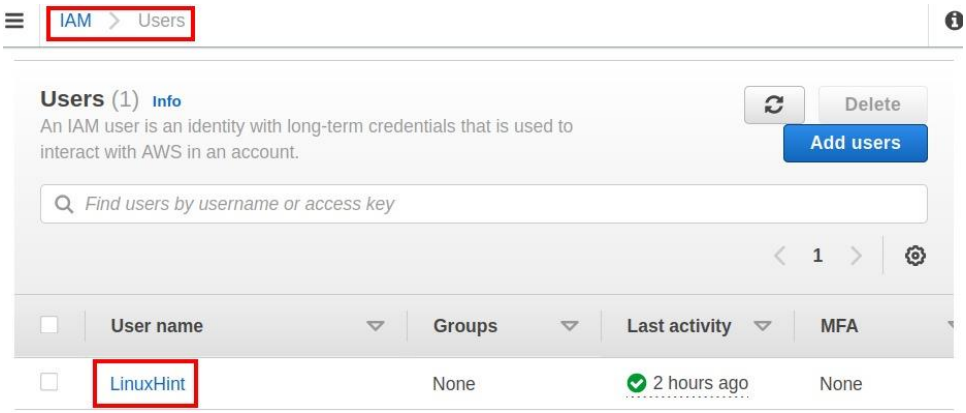


As an IAM administrator, we will create a policy and then attach it to the IAM user. This policy will enable our IAM users to:

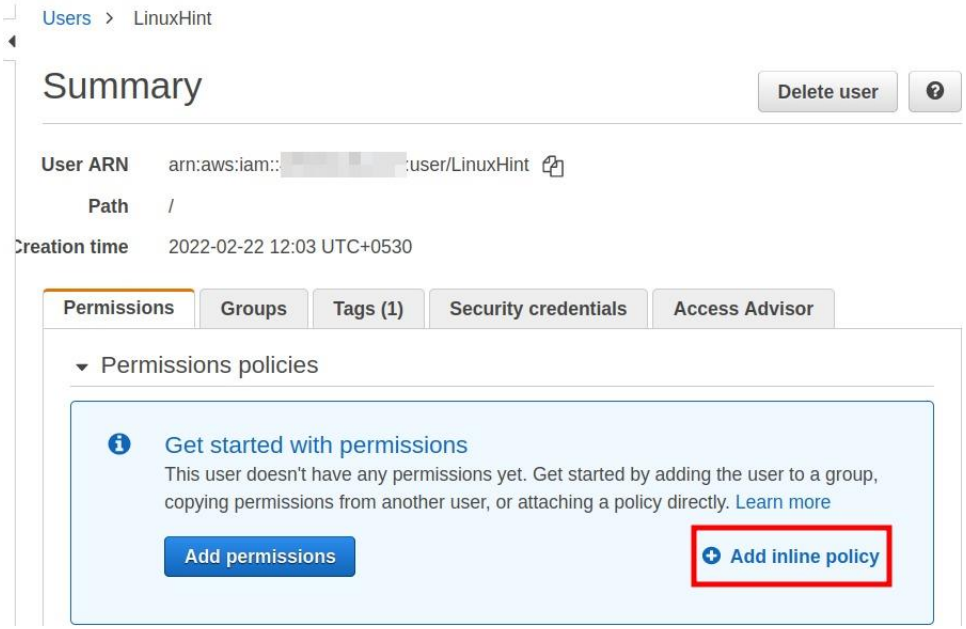
- **Create database**
- **Delete database**
- **Describe database**
- **Start database**
- **Stop database**

For the above operation, we will add an identity-based policy called Inline policy. This inline policy is a set of minimum permission set for the above-specified database operation. Now follow the instructions below:

Step 1. Go to the AWS IAM console of the root Account and click ‘Users’ and choose the target user from the list(‘LinuxHint’ in our case):



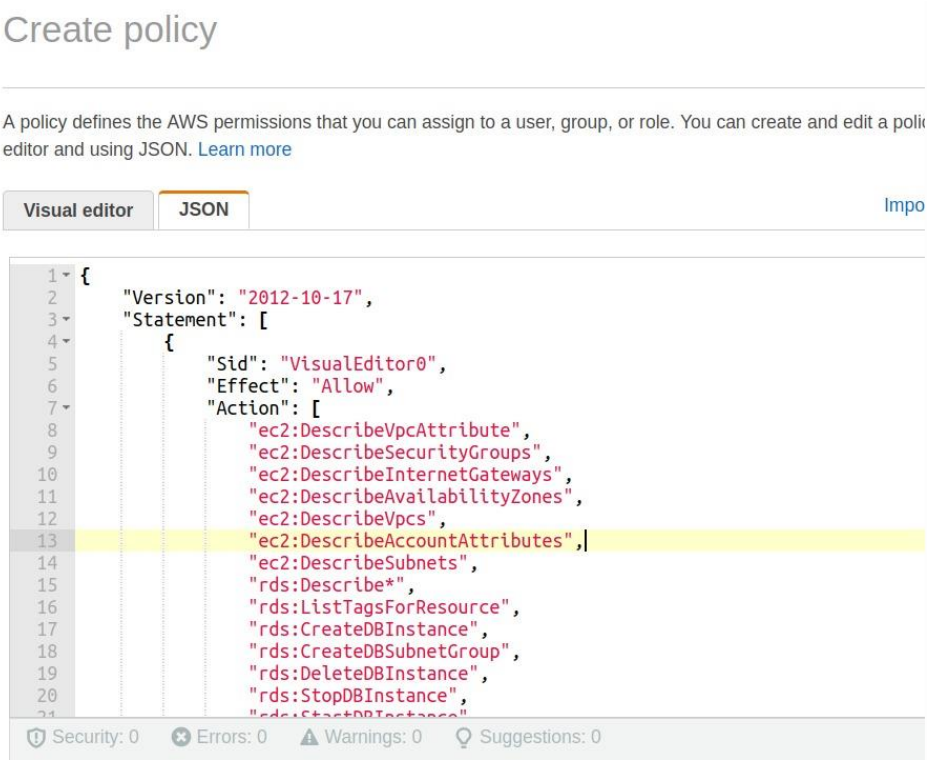
Step 2. On the new page, we can see that there are no policies attached to the IAM user. Click on ‘Add inline policy’ as shown below:



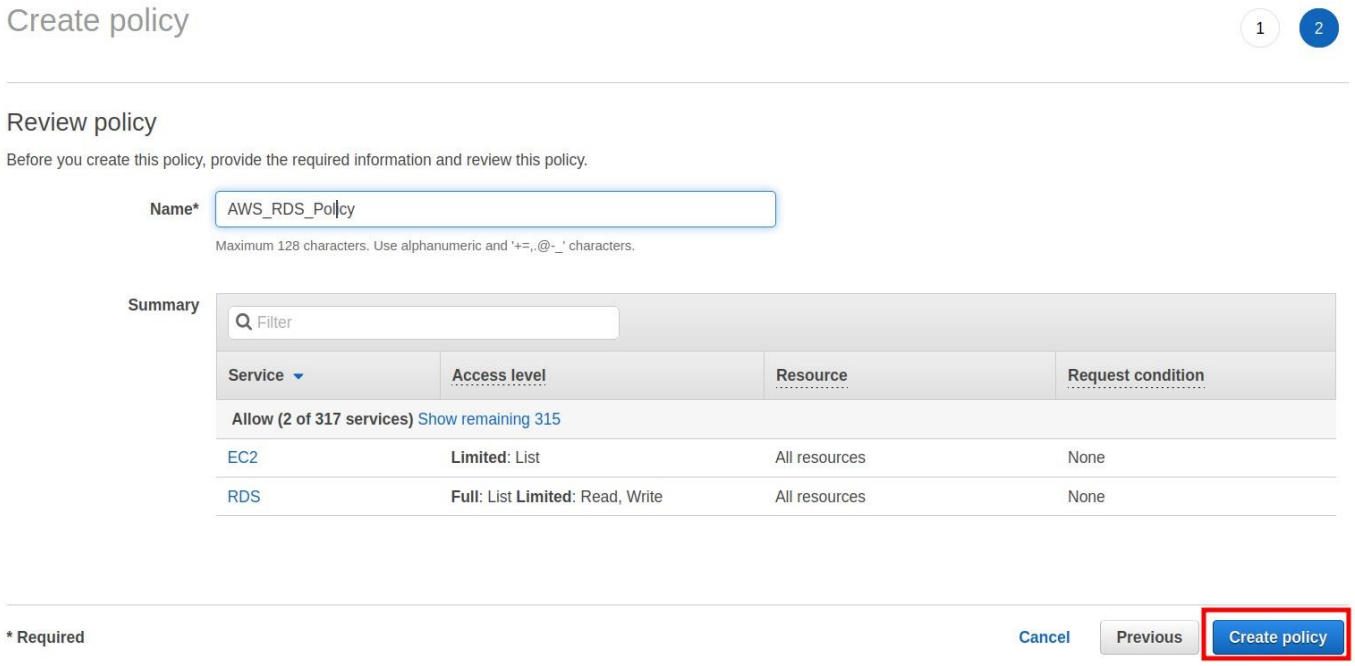
Step 3. A new wizard named as ‘Create policy’ will appear where you have to select the JSON tab and paste the below code there:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSubnets",
                "rds:Describe*",
                "rds:ListTagsForResource",
                "rds:CreateDBInstance",
                "rds:CreateDBSubnetGroup",
                "rds:DeleteDBInstance",
                "rds:StopDBInstance",
                "rds:StartDBInstance"
            ],
            "Resource": "*"
        }
    ]
}
```

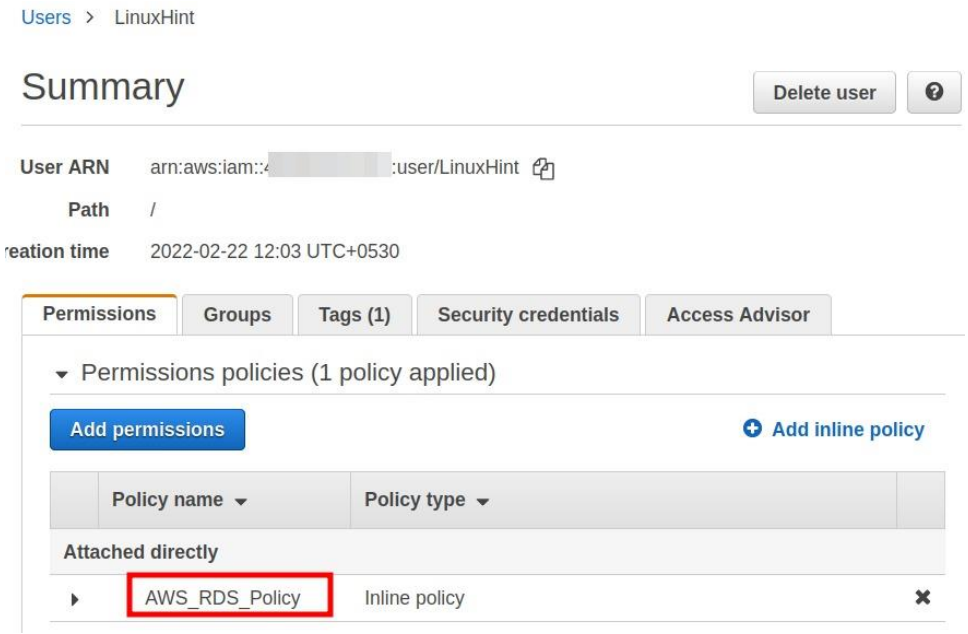
Step 4. Now click the ‘Review policy’ button at the bottom:



Step 5. Give a suitable name to your policy and click the “Create policy’ button:

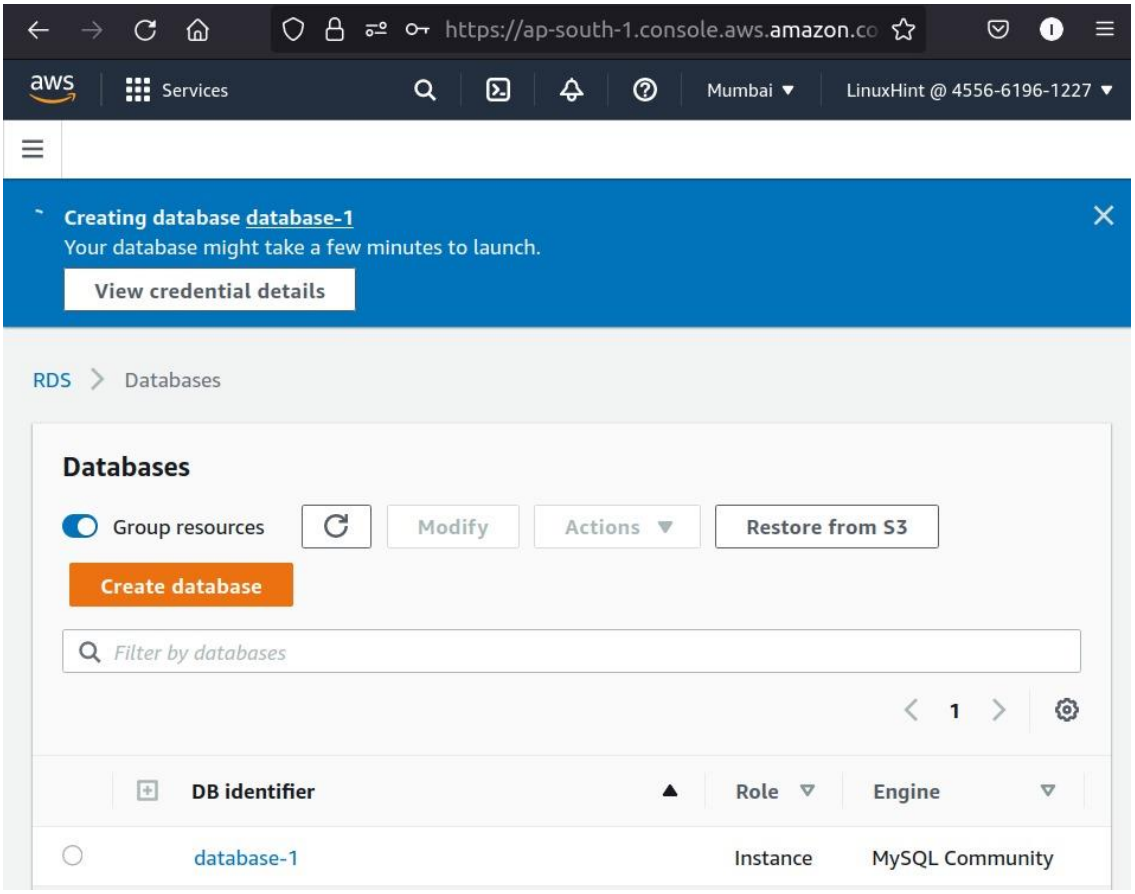


The above inline policy can now be seen under the permissions tab:



Now we can create and manage an RDS database through an IAM user. To check this, head back to the RDS console of the IAM user and again try to launch an RDS

DB instance. This time we can launch the database easily under the ‘Standard create’ option of the RDS launch wizard.



Question 4. Why do we prefer not using root account?

Ans. Using the AWS root account means that there is potential for its compromise. In particular ,iSEC noticed that AWS customers who use the AWS root account tend to do the following:

1.Share credentials between employees.

2.Disable Multi-Factor Authentication (MFA) for convenience.

Shared credentials, aside from increasing the risk of compromise during the sharing process, render credential rotation impractical due to the need for the newly- generated secret to be known by multiple parties.

Sharing the AWS root account also undermines any effort towards using IAM and leveraging the fine-grained access controls it offers.

Finally, shared credentials result in loss of the attribution ability, which makes auditing harder and may prevent successful investigation.

Question 5. How to revoke policy for an IAM user ?Ans. We can delete a customer managed policy to remove it from your AWS account. You cannot delete AWS managed policies.

To delete a customer managed policy (console)

- Sign into the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
- In the navigation pane, choose **Policies**.
- Select the check box next to the customer managed policy to delete. You can use the search box to filter the list of policies.
- Choose **Actions**, and then choose **Delete**.
- Confirm that you want to delete the policy, and then choose **Delete**.