Laboratório de Desafios – Controlando o Acesso à Conta da AWS Usando o IAM

1.) Desafio nº 1

Foi criado o grupo de acessos no IAM AppDevelopers com duas políticas associadas a ele:

- AmazonEC2ReadOnlyAccess
- AWSCloud9EnvironmentMember

Posteriormente foi criado o usuário Nikhil e foi adicionado ao grupo AppDevelopers.

Logada como Sofia foi criado e compartilhado com o usuário Nikhil o ambiente do Cloud9

Logando com o usuário Nikhil foi efetuado o teste de restart da instância aws-cloud9-DEVCafeServer, porém Nikhil não tinha permissão para fazer ações nas instâncias EC2. As permissões de Nikhil era apenas visualização das instâncias EC2 e acesso de RW ao ambiente do Cloud9, permitido pela política AWSCloud9EnvironmentMember.

Logada Nikhil foi efetuado o teste de alteração de arquivos na página index.php, foi alterado o cabeçalho da página.

Foi efetuado um teste no site no ambiente de desenvolvimento, clicando no Menu e um erro de conexão com banco de dados ocorreu, por conta de falta de permissão do usuário root.

Ainda como Nikhil após o erro do site de desenvolvimento tentei verificar os parâmetros no serviço de Parameter Store já que as credencias de banco são gravadas nesse serviço, porém Nikhil não tem permissão para visualizar o Parameter Store.

2.) Desafio nº 2

Foi verificado se o erro que ocorria no site de desenvolvimento acontecia no site de produção, produção estava funcionando corretamente.

Então logada como Sofia foi criado um grupo de acessos no IAM DBAdministrators com as seguintes políticas associadas a ele:

- AmazonRDSReadOnlyAccess
- AmazonSSMFullAccess

Posteriormente foi criado o usuário Olivia e foi adicionada ao grupo DBAdministrators para resolver o problema do site de desenvolvimento.

Logada como Olivia foi verificado se a instância de banco de dados de RDS estava disponível, estava ok.

Como Olivia houve a tentativa de ver as instâncias EC2, porém Olivia não tinha as políticas de visualização de instâncias EC2 associadas ao seu usuário.

Logada como Sofia foi adicionado ao grupo DBAdministrators as políticas AmazonEC2ReadOnlyAccess e IAMReadOnlyAccess, grupo ao qual Olivia está adicionada, sendo assim Olivia passou a ter o acesso de visualização nas instâncias de EC2.

Como Sofia foi observado os acessos de Olivia na console do IAM Access Advisor.

Olivia com o acesso de visualização das instâncias de EC2 conseguiu revisar as políticas da role associada à instância de EC2 e ter certeza que a instância tinha acesso ao repositório de parâmetros.

O problema de acesso ao banco de dados no site de desenvolvimento estava relacionado com o fato de o valor dbUser estar errado no repositório de parâmetros, com a alteração efetuada por Olivia o site de desenvolvimento passou a funcionar.

3.) **Desafio nº 3**

Foi testada a página IAM Policy Simulator para o usuário Olivia, verificando os possíveis acessos através da seleção das políticas e execução das mesmas.

Posteriormente foi utilizado o Visual Editor para criação de políticas mais restritivas para o grupo DBAdministrators em relação aos serviços de EC2, por conta limitações do lab não foi possível finalizar a criação da política, mas já existia uma política criada com as permissões necessárias para limitar permissões aos serviços do EC2.

Foi associado ao grupo DBAdministrators a política LimitedIamPolicy e desassociada a política IAMReadOnlyAccess.

Com o usuário Olivia foi testado as novas permissões do grupo DBAdministrators, Olivia continua com permissões aos serviços do EC2, porém muito mais limitadas que as permissões anteriores.

Observação: O questionário proposto no lab foi respondido.