Temporary Credentials

1. Introduction to IAM Roles

- **Definition**: IAM roles provide permissions that allow AWS resources like EC2 instances to securely access other AWS services without requiring user-specific credentials.
- **Benefits of IAM Roles**:
  - **Enhanced Security**: By avoiding hard-coded credentials, IAM roles reduce security risks.
  - **Ease of Management**: Centralized permissions for easy modification or revocation.
  - **Fine-Grained Access Control**: Limit access to specific resources, promoting the principle of least privilege.

2. How IAM Roles Work with EC2 Instances

- **Role-Based Access**: An IAM role can be assigned to an EC2 instance, allowing it to assume permissions and make API requests to AWS services like S3.
- **Temporary Credentials**: IAM roles provide temporary credentials that rotate automatically, reducing the need for long-term access keys.

3. Step-by-Step Guide: Setting Up IAM Roles with EC2 to Access S3

1. **Create an IAM Role**:
   - In the **IAM Console**, create a new role and select **EC2** as the trusted entity.
   - Attach a policy, such as **AmazonS3ReadOnlyAccess, AmazonS3FullAccess** or a custom policy.
2. **Attach the IAM Role to an EC2 Instance**:
   - In the **EC2 Console**, select the instance, go to **Actions** > **Security** > **Modify IAM role**.

   - Choose the role you created and attach it to the instance.
3. **Test Access**:
   - Connect to the EC2 instance and use the AWS CLI to verify access.

4. Best Practices

- **Apply Least Privilege**: Only assign the minimum permissions necessary.
- **Use Managed Policies**: AWS-managed policies are maintained and updated by AWS.
- **Monitor Role Usage**: Use **CloudTrail** to track role usage and adjust permissions accordingly.

5. Resources and Further Reading

- AWS Guide to Switching Roles with EC2: Detailed instructions on switching roles within EC2.
- IAM Roles for Amazon EC2: Overview and instructions for attaching IAM roles to EC2 instances.

Conclusion

Setting up IAM roles with EC2 enhances security, simplifies management, and ensures that your EC2 instances have secure access to other AWS services.