**Updated 10 Hands-On Assignments for AWS IAM**

1. **Create a New IAM User**
   * Create a new IAM user with programmatic access. Assign permissions to access a specific S3 bucket.
2. **Implement IAM Groups**
   * Create an IAM group for developers, attach a policy allowing full access to EC2, and add users to the group.
3. **Set Up a Password Policy**
   * Configure a password policy requiring specific length, complexity, and expiration settings for IAM users.
4. **Create a Custom IAM Policy**
   * Write a custom policy in JSON format that allows access to DynamoDB but denies delete operations.
5. **Assign IAM Roles to EC2 Instances**
   * Create an IAM role to allow an EC2 instance to access an S3 bucket. Attach the role to an existing instance.
6. **Enable Multi-Factor Authentication (MFA)**
   * Enable MFA for an IAM user and test logging in using both password and MFA code.
7. **Audit IAM Users**
   * List all IAM users in your account and identify which ones haven’t used their credentials in the past 90 days.
8. **Restrict IP Access Using IAM Policies**
   * Create a policy that allows access to AWS services only from a specific IP address range.
9. **Create and Manage IAM Roles**
   * Create an IAM role to allow a Lambda function to write logs to CloudWatch. Test the role by deploying a sample Lambda function.
10. **Integrate IAM Roles with Groups**
    * Create a group for database administrators. Attach a role that grants access to RDS databases and add users to the group.

**Updated 10 Hands-On Assignments for AWS S3 Bucket**

1. **Create an S3 Bucket**
   * Create a new S3 bucket with versioning enabled and upload a sample file to the bucket.
2. **Set Bucket Policies**
   * Configure a bucket policy that allows read-only access to objects for a specific IP range.
3. **Enable Bucket Logging**
   * Set up server access logging for an S3 bucket and specify a target bucket for storing the logs.
4. **Implement Object Lifecycle Management**
   * Create a lifecycle policy to transition objects to the Infrequent Access storage class after 30 days and delete them after 90 days.
5. **Set Up Static Website Hosting**
   * Use an S3 bucket to host a static website. Upload an HTML file and test the website URL.
6. **Use Presigned URLs**
   * Generate a presigned URL to grant temporary access to an object in an S3 bucket and test it.
7. **Restrict Access Using Bucket ACLs**
   * Configure Access Control Lists (ACLs) to grant access to a specific AWS account.
8. **Enable Cross-Origin Resource Sharing (CORS)**
   * Set up a CORS policy to allow a web application to access objects in your S3 bucket.
9. **Encrypt Bucket Data**
   * Enable server-side encryption for an S3 bucket using AWS-managed keys (SSE-S3).
10. **Replicate Objects Across Buckets**
    * Configure S3 Cross-Region Replication to replicate objects from one bucket to another in a different region.

These updates ensure comprehensive coverage of **IAM groups** and **roles**, alongside core S3 features for a hands-on learning experience.