Acme Manufacturing Cloud Migration: Runbooks

These runbooks provide operational procedures for common tasks and troubleshooting during the Acme Manufacturing cloud migration. They are intended as quick references for the team. Always refer to official AWS documentation for complete details and best practices.

I. Common Tasks:

A. EC2 Instance Launch:

1. **Verify Instance Type:** Confirm the correct AMI (Amazon Machine Image), instance type (e.g., t2.micro, m5.large), and key pair are selected.
2. **Security Group Assignment:** Ensure the correct security group (e.g., Acme-Web-SG, Acme-Database-SG) is assigned, allowing only necessary inbound and outbound traffic.
3. **Storage Configuration:** Define the appropriate storage (EBS volume type and size) based on the application's needs.
4. **Launch Instance:** Click "Launch Instances" and monitor the instance's status until it reaches the "running" state.
5. **Post-Launch Checks:** Verify network connectivity, SSH access, and application functionality.

B. S3 Bucket Creation and Data Upload:

1. **Bucket Naming:** Choose a globally unique bucket name (following S3 naming conventions).
2. **Region Selection:** Select the appropriate AWS region for optimal latency and data locality.
3. **Access Control:** Configure bucket policies and ACLs to restrict access based on the principle of least privilege (only authorized users and services should have access).
4. **Encryption:** Enable server-side encryption (SSE) with AWS KMS-managed keys for data encryption at rest.
5. **Versioning:** Enable versioning to protect against data loss and accidental deletion.
6. **Data Upload:** Utilize the AWS Management Console, AWS CLI, or other tools for secure and efficient data transfer. Verify data integrity post-upload.

C. RDS Instance Creation and Data Migration:

1. **Instance Selection:** Choose the appropriate DB engine (e.g., MySQL, PostgreSQL), instance class, and storage type based on the application's requirements.
2. **Security Group Configuration:** Assign the Acme-Database-SG security group to control database access.
3. **IAM Role:** Ensure the correct IAM role is assigned to manage database access.
4. **Data Import:** Utilize AWS DMS or other tools to migrate data securely and efficiently from the on-premises database to the RDS instance. Verify data integrity post-migration.

5. **Connection Testing:** Test the database connection from the application server.

II. Troubleshooting:

A. EC2 Instance Connectivity Issues:

1. **Security Group Check:** Verify that the inbound rules of the security group allow SSH access from your IP address.
2. **Network Configuration:** Ensure that the instance's network interface (ENI) is associated with a subnet and that the subnet has appropriate routing.
3. **Key Pair Validation:** Confirm that you're using the correct key pair to connect via SSH.
4. **Instance Status:** Check the instance's status in the EC2 console. If stopped, start the instance.
5. **DNS Resolution:** Verify that the instance can resolve DNS names.

B. S3 Data Upload Failures:

1. **Bucket Policy Review:** Check the bucket's policy to ensure it allows uploads from the source.
2. **IAM Permissions:** Ensure that the IAM user or role has the necessary permissions to upload data to the bucket.
3. **Network Connectivity:** Verify network connectivity between the source and the S3 bucket.
4. **File Size Limits:** Check if the file size exceeds the allowed limit.
5. **Error Messages:** Carefully review any error messages provided by the upload tool.

C. RDS Connection Issues:

1. **Security Group Check:** Verify that the inbound rules of the security group allow connections from the application server.
2. **Endpoint Verification:** Confirm that you're using the correct RDS endpoint.
3. **IAM Role Validation:** Verify that the IAM role has the necessary permissions to access the database.
4. **Database Credentials:** Ensure you're using the correct database username and password.
5. **RDS Instance Status:** Check if the RDS instance is running and available.

III. Documentation:

All actions performed using these runbooks should be meticulously documented, including dates, times, user, steps taken, and outcomes. This documentation is critical for auditing, troubleshooting, and future reference.

These runbooks are designed to be a quick reference guide. For more detailed information, please refer to the official AWS documentation. Always prioritize security and ensure that all actions are performed in accordance with best practices.