Acme Manufacturing Cloud Migration: Pilot Migration Phase

This document provides step-by-step instructions for the Pilot Migration phase of the Acme Manufacturing cloud migration project. The goal of this phase is to validate the migration process on a small scale before migrating critical applications. This phase will involve migrating a small set of low-impact applications. Remember to always consult the official AWS documentation for the most up-to-date information and best practices.

I. Application Selection:

1. **Identify Pilot Applications:** Select a small set of low-impact applications for migration. These applications should be chosen based on their size, complexity, dependencies, data volume, and business criticality. Prioritize applications with minimal dependencies on other systems. A good choice might be applications that have minimal impact on business operations if a rollback is necessary.
2. **Document Dependencies:** Carefully document all application dependencies, including databases, external services, and other systems.
3. **Data Assessment:** Perform a thorough assessment of the data associated with each pilot application. Identify any data quality or compliance issues that may need to be addressed before migration.

II. Preparation:

A. AWS Environment Review (Yanga):

1. **VPC Configuration:** Verify the VPC configuration, ensuring sufficient resources (subnets, security groups, NAT gateway) are available. Check routing table configurations to confirm connectivity to both the internet and on-premises network if needed.
2. **IAM Roles:** Confirm that appropriate IAM roles have been created for all services involved in the pilot migration, granting only necessary permissions.
3. **Security Groups:** Verify that security groups have been properly configured to restrict access based on the principle of least privilege. Review inbound and outbound rules for each application.
4. **Storage Configuration:** Ensure that sufficient storage (S3, RDS, DynamoDB, EFS, etc.) is available for the pilot applications and their data.

B. Application Packaging (Tsakani):

1. **Deployment Artifacts:** Prepare deployment artifacts for each pilot application, ensuring all necessary dependencies and configurations are included. This is crucial to prevent issues during the migration.

C. Data Preparation (Bushy):

1. **Data Extraction:** Extract a representative subset of data for each pilot application. The data subset should be sufficient to test the migration process but minimize data volume to reduce migration time.
2. **Data Transformation:** If necessary, transform the data to be compatible with the target database or storage system in AWS.
3. **Data Validation:** Validate the extracted data for accuracy and completeness.

III. Migration Execution:

A. Application Migration (Tsakani):

1. **Deployment:** Deploy each pilot application to its designated environment in AWS (EC2, ECS, EKS, or Lambda, as appropriate). Follow the deployment procedures detailed in the application-specific deployment documents.
2. **Post-Deployment Checks:** Verify that each application is running correctly and all its functions are working as expected.

B. Data Migration (Bushy):

1. **Data Loading:** Migrate the prepared data subset to the designated database or storage service in AWS.
2. **Data Validation:** Verify the data integrity after the migration.

IV. Testing and Validation:

A. Functional Testing (Tsakani):

1. **Test Cases:** Execute a comprehensive set of test cases for each pilot application to ensure that all core functions are working as expected in the AWS environment.
2. **Defect Tracking:** Log and track any defects or issues identified during testing.

B. Performance Testing (Yamkelani):

1. **Load Testing:** Conduct load tests to assess the performance of the migrated applications under various load conditions.
2. **Resource Monitoring:** Monitor resource utilization (CPU, memory, network) to identify potential bottlenecks.

C. Security Testing (Lusanda):

1. **Vulnerability Assessment:** Conduct vulnerability scans to identify any security weaknesses or vulnerabilities.

2. **Access Control Verification:** Verify that access control mechanisms (security groups, IAM roles) are functioning correctly and that access is appropriately restricted based on the principle of least privilege.

D. Data Validation (Bushy):

1. **Data Integrity Checks:** Verify that the data migrated to AWS is accurate, complete, and consistent with the source data.

V. Documentation:

1. **Detailed Steps:** Document all steps taken during the migration and testing processes, including commands executed, configurations applied, and any issues encountered.
2. **Test Results:** Document all test results, including performance metrics and any identified issues.
3. **Lessons Learned:** Document any lessons learned during this phase, which will be valuable for the gradual migration phase.

This document provides a high-level overview. More detailed instructions will be provided for each application. Remember to prioritize security, and thoroughly test at each step. Rollback plans should be defined and tested for each application before proceeding to the migration phase.