Acme Manufacturing Cloud Migration: AWS Architectural Framework

This document outlines the AWS architecture designed for Acme Manufacturing's cloud migration, illustrating the key services, their roles, and the phased approach to implementation.

2. Phased Migration Approach

The migration follows a three-phase approach:

- **Phase 1: Pilot Migration:** Identifies candidate applications, configures initial AWS services, and tests the migration process.
- **Phase 2: Gradual Migration:** Gradually migrates applications to AWS, leveraging chosen services.
- **Phase 3: Optimization & Automation:** Optimizes processes and implements automation for operational excellence and cost savings.

3. Networking & Connectivity

- **On-Premises:** Acme's existing on-premises infrastructure is connected to AWS using a dedicated, high-bandwidth connection (AWS Direct Connect).
- **VPC:** A secure, isolated virtual private cloud (VPC) in AWS is created to host the migrated resources. This provides network segmentation and control.
- **NAT Gateway:** A Network Address Translation (NAT) Gateway is deployed within the VPC, allowing instances in private subnets to access the internet while maintaining their private IP addresses.
- **Security Groups:** Security groups enforce a layered security model, controlling network traffic to and from individual EC2 instances.

4. Compute & Application Hosting

- **EC2 (Simple Migration):** Acme's on-premises applications are initially migrated to EC2 instances for a straightforward transition.
- **ECS (Containerized Applications):** Applications are containerized and deployed on Amazon Elastic Container Service (ECS) for greater scalability and flexibility.
- **EKS (Complex Containerized Workloads):** Amazon Elastic Kubernetes Service (EKS) manages complex containerized applications, providing high-level orchestration and scalability.
- **Lambda (Serverless Functions):** Serverless computing is leveraged with AWS Lambda for event-driven processing, automating tasks, and simplifying code execution.

5. Data Storage & Backup

- **S3:** Amazon Simple Storage Service (S3) serves as the primary storage for objects, including data backups and archives.
- **RDS:** Amazon Relational Database Service (RDS) manages relational databases, providing a managed environment for SQL databases.
- **DynamoDB:** Amazon DynamoDB manages NoSQL databases, providing a scalable and high-performance solution for NoSQL data needs.
- **EBS:** Amazon Elastic Block Storage (EBS) provides persistent block storage volumes attached to EC2 instances for local data access.
- **Glacier:** Amazon Glacier securely stores long-term data archives for cost-effective data retention and disaster recovery.

6. Performance & Optimization

- **CloudFront:** Amazon CloudFront is a content delivery network (CDN) that distributes website content globally, reducing latency and improving user experience.
- **ElastiCache:** Amazon ElastiCache implements in-memory caching, reducing database load and boosting application response times, especially for frequently accessed data.
- **Route 53:** Amazon Route 53 resolves domain names and manages DNS records for optimal performance and availability.
- **CloudWatch:** Amazon CloudWatch monitors application performance, resource utilization, and security events in real-time, enabling proactive troubleshooting and resource optimization.

7. Security & Compliance

- **SecurityHub:** Amazon SecurityHub centralizes security management, providing a comprehensive view of security posture and threat detection.
- **IAM:** AWS Identity and Access Management (IAM) controls access to AWS resources, granting granular permissions to users and applications.
- **KMS:** AWS Key Management Service (KMS) manages encryption keys for data at rest and in transit, ensuring data confidentiality and compliance.
- **GuardDuty:** Amazon GuardDuty detects malicious activity and threats across the AWS environment, automating security monitoring and alerting.
- **Inspector:** Amazon Inspector scans for security vulnerabilities in EC2 instances and container images, proactively mitigating risks.
- **WAF:** AWS Web Application Firewall (WAF) protects web applications from common web exploits.

8. Operational Excellence

- **CloudFormation:** AWS CloudFormation automates infrastructure provisioning and management, ensuring consistency and repeatability of deployments.
- **CloudTrail:** AWS CloudTrail provides a comprehensive audit trail, logging all API calls and events, enabling security monitoring and compliance.

- **Systems Manager:** AWS Systems Manager automates system administration tasks, simplifying operations and reducing errors.

9. Legend:

- **aws:** Represents an AWS Service.
- **Information:** Describes the purpose or function of the service.

Conclusion:

This AWS architectural framework provides a detailed overview of Acme Manufacturing's cloud migration strategy. The chosen services, their interconnectedness, and the phased approach are designed to deliver a secure, scalable, and cost-efficient cloud environment. By implementing this framework, Acme Manufacturing will benefit from increased agility, reduced operational overhead, and a more robust IT infrastructure to support future business growth.

Further Notes:

- This document serves as a high-level overview. Detailed configuration and implementation steps are not included.
- It is recommended to conduct regular security assessments and updates to ensure ongoing security and compliance within the AWS environment.