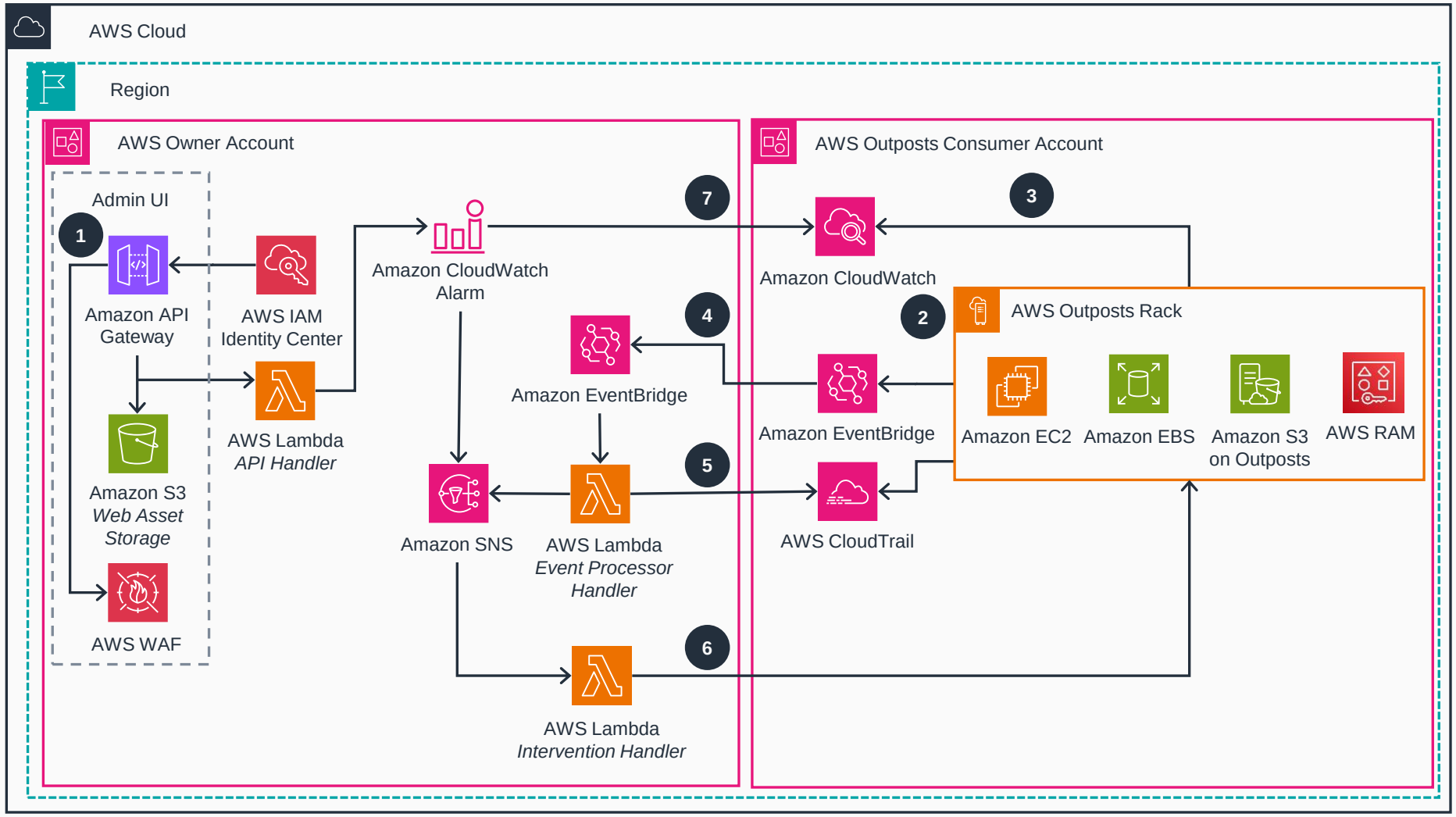
# Guidance for Multi-Account Outposts Operations on AWS

This architecture diagram demonstrates how to set soft and hard limits on Amazon EC2 resources for member accounts that share an AWS Outposts rack.




1. Admin users authenticate via **AWS IAM Identity Center**. The **AWS Outposts** owner account hosts the web UI and the API using **Amazon API Gateway**. **AWS Web Application Firewall (AWS WAF)** provides IP-based access control. The **AWS Lambda** API Handler executes changes in the UI.

2. **AWS Resource Access Manager (AWS RAM)** shares the services in the **AWS Outposts** rack with the Consumer Account. The controlled resources on the **Outposts** rack can include services like **Amazon Elastic Compute Cloud (Amazon EC2)**, **Amazon Elastic Block Store (Amazon EBS)**, and **Amazon Simple Storage Service (Amazon S3)**.

3. The Customer Account **Amazon CloudWatch** reads **CloudWatch** Alert thresholds from the Consumer Account and writes them to a centralized alert configuration.

4. **Amazon EventBridge** powers the event management system, actively routing service notifications such as 'an EC2 instance has started'.

5. When triggered by an event, the Event Processor Handler **Lambda** function collects real-time usage data from the consumer account. This **Lambda** function then evaluates this data against **CloudWatch** alert thresholds to determine if automated intervention is necessary.

6. The Event Processor Handler **Lambda** function sends a message on the **Amazon Simple Notification Service (Amazon SNS)** Alert Topic to the Intervention Handler Lambda function, which performs remedial actions, as applicable.

7. **CloudWatch** triggers an alert when an **Outposts** resource crosses a set threshold.

*Reviewed for technical accuracy August 21, 2025*



**AWS Reference Architecture**