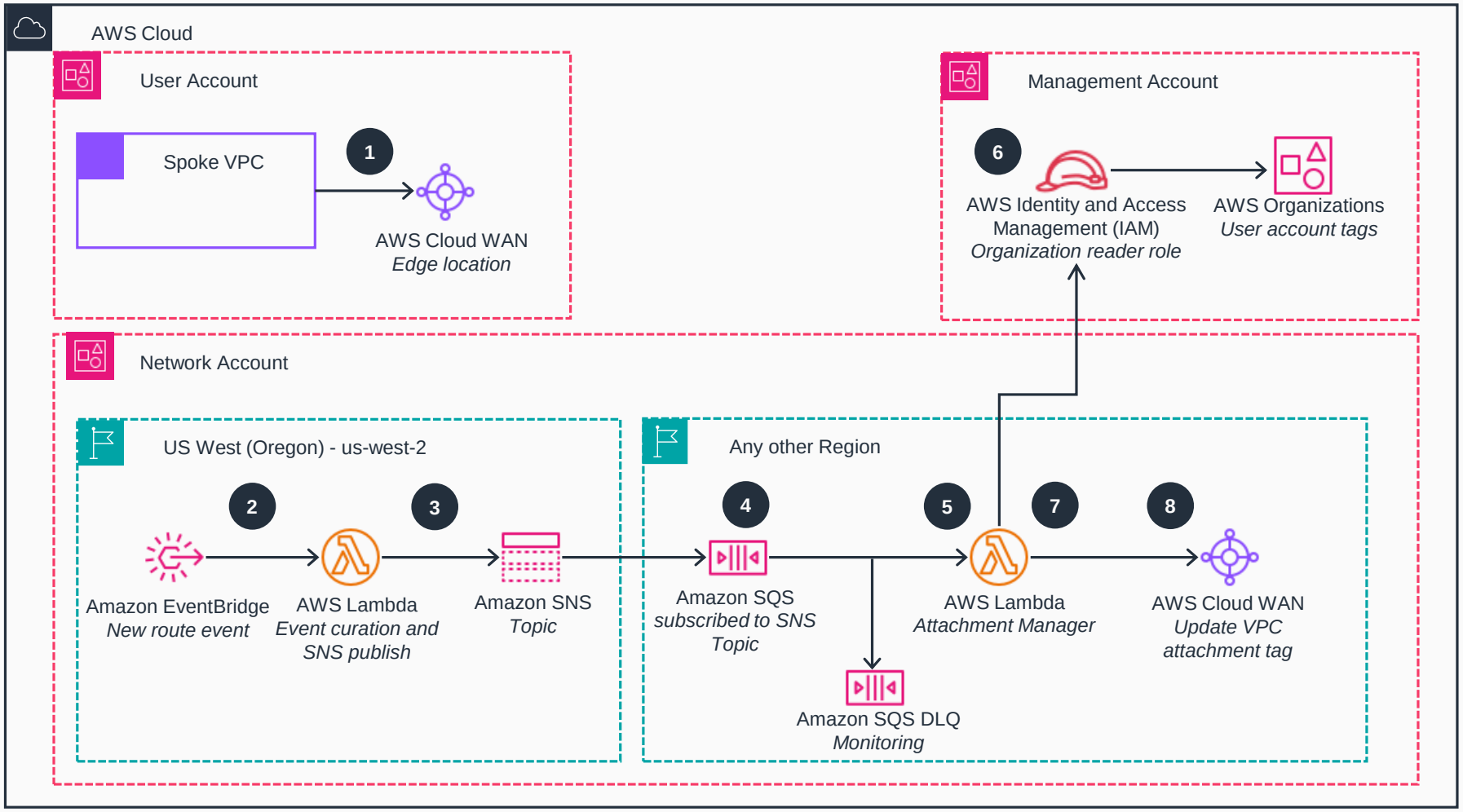
Guidance for Attachment Management to AWS Cloud WAN

This architecture diagram shows how to perform automated and secure Attachment Management to AWS Cloud WAN networks.
Steps 1-4 are outlined below. For details on steps 5-8, refer to the next slide.



1. In a user account, a Spoke **Amazon Virtual Private Cloud** (Amazon VPC) is attached to a shared **AWS Cloud WAN** edge location. By default, the attachment is moved to a quarantine network segment.

2. Once the Spoke **Amazon VPC** CIDR ranges are learned, a *New route event* (or topology change) is generated by AWS Network Manager. The event is processed by **Amazon EventBridge**, which sends it to the *Event curation and SNS publish* **AWS Lambda** function for curation.

3. The *Event curation and SNS publish* **Lambda** function parses the event and publishes it to an **Amazon Simple Notification Service** (Amazon SNS) topic. It's published with enriched attributes, such as *attachmentArn and attachmentId.*

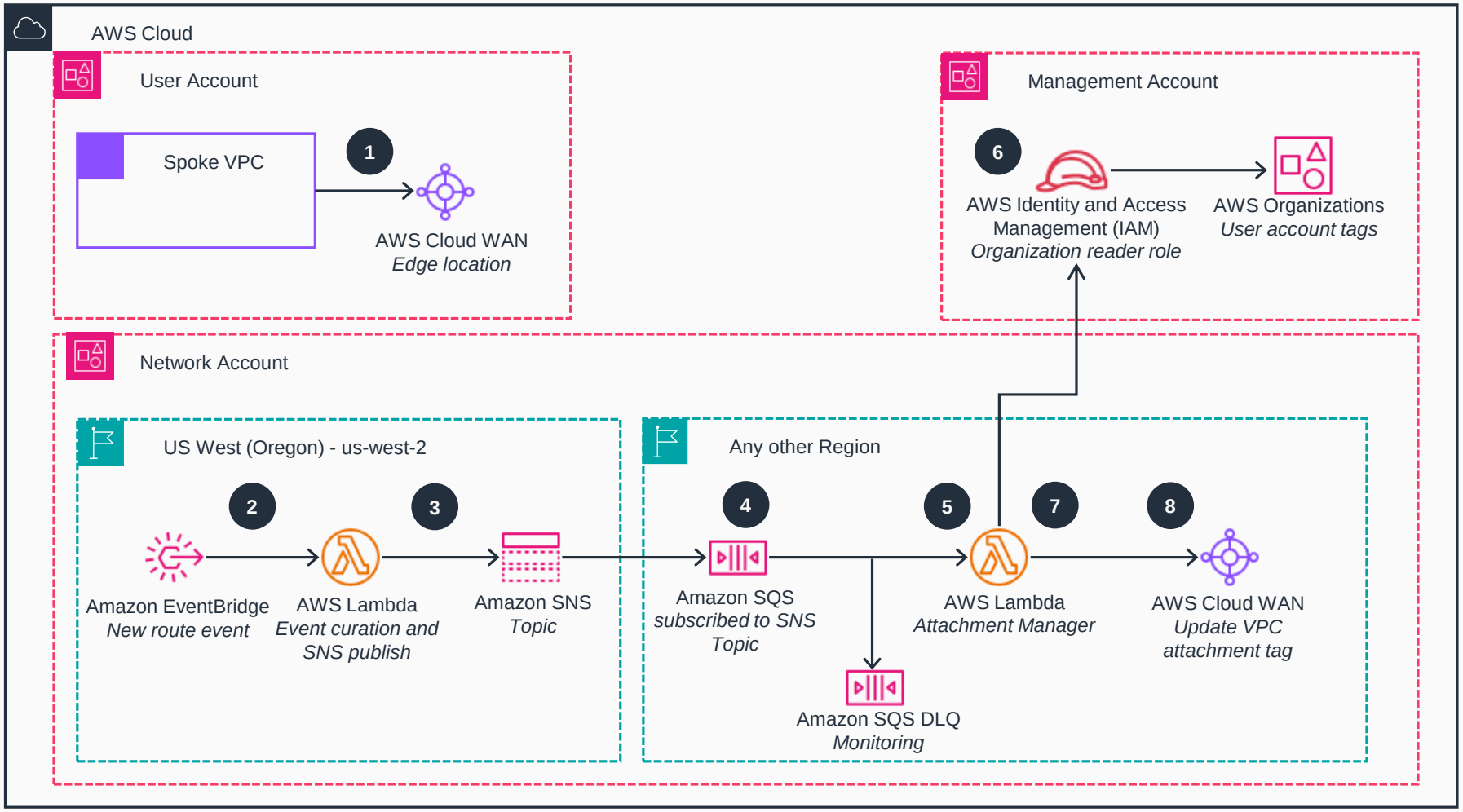
4. An **Amazon Simple Queue Service** (Amazon SQS) deployed in another AWS Region has a queue subscribed to the **Amazon SNS** topic and filters events of interest based on their message attributes. A Dead Letter Queue (DLQ) is also configured for monitoring and troubleshooting.

Reviewed for technical accuracy July 3, 2024

AWS Reference Architecture

Guidance for Attachment Management to AWS Cloud WAN

Steps 5-8



5 The *Attachment Manager* **Lambda** function reads events from the **Amazon SQS** queue to perform the attachment admission to the network.

6 The *Attachment Manager* **Lambda** function assumes a role in the Management Account. This role is used to read the segment and account tags of the user account that created the **Amazon VPC** attachment to **AWS Cloud WAN**. A '*route-domain*' tag will identify a network segment to which the *User account* belongs (such as production, testing, and development).

7 This Guidance also provides an option to package the Plan for IP address provisioning of the global network in the *Attachment Manager* **Lambda** function. In that case, the *New route event* being advertised is also verified for adherence to the plan for IP address provisioning.

8 If the evaluation logic is successful, the *Attachment Manager* **Lambda** function will tag the Spoke **Amazon VPC** attachment with the correct tag to ensure it is admitted to the correct **AWS Cloud WAN** network segment. Otherwise, the attachment will be deleted.

Reviewed for technical accuracy July 3, 2024

AWS Reference Architecture