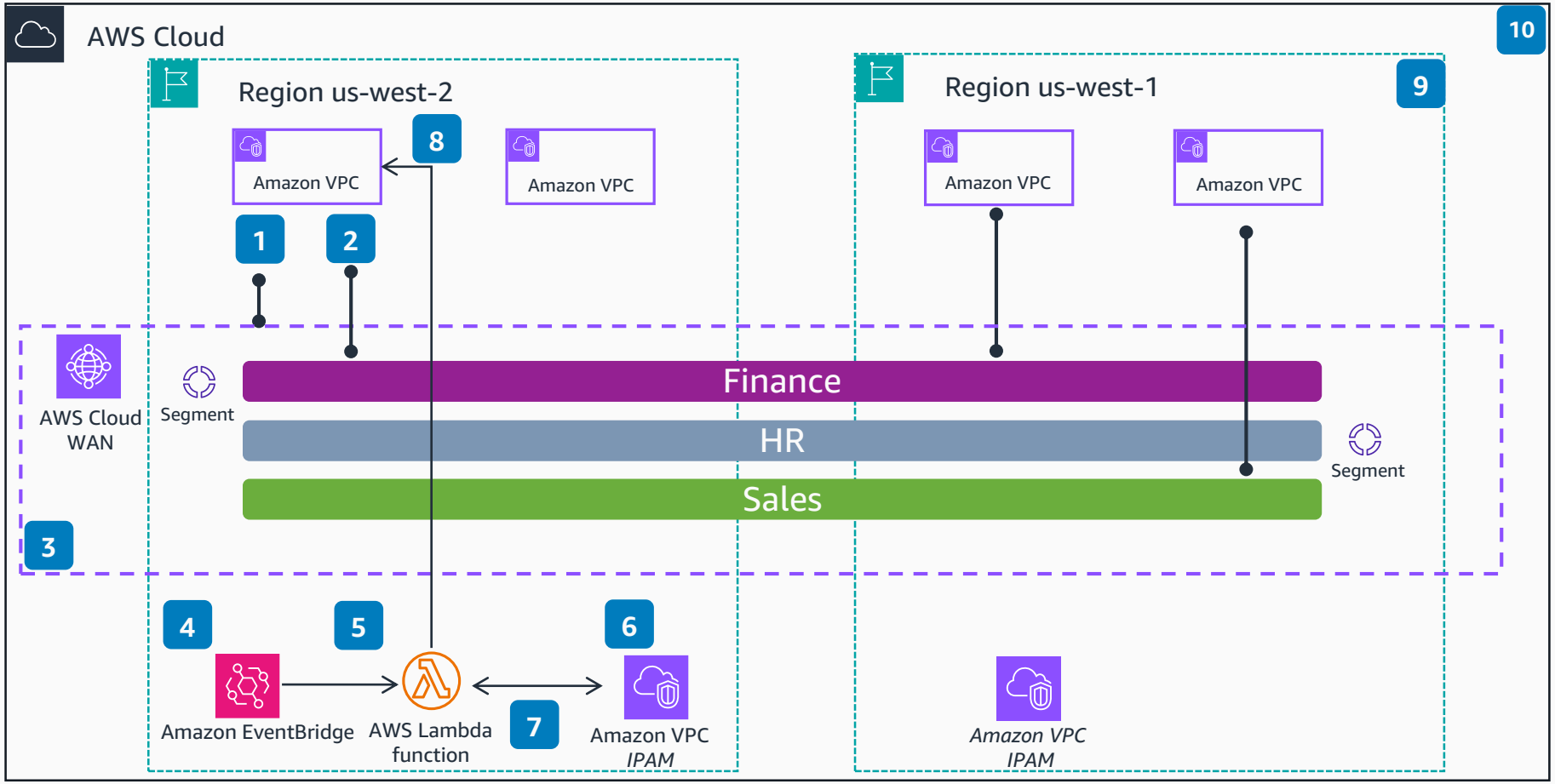
Guidance for Automating Amazon VPC Routing in a Global AWS Cloud WAN Deployment

This diagram shows how to create an end-to-end global routing cloud network. You can deploy an Amazon Virtual Private Cloud (Amazon VPC) in multiple AWS Regions and automate your global Amazon VPC routing with this event-driven architecture.



1. A new **Amazon Virtual Private Cloud** (Amazon VPC) is attached to **AWS Cloud WAN**.
2. A network administrator attaches metadata (for example: a key-value pair tag) on the **Amazon VPC** attachment. This ensures the **Amazon VPC** attachment lands in the right **AWS Cloud WAN** segment. For this Guidance, the key-value pair tag must be in the 'department:<department-name>' format. For example, department:Finance.
3. **AWS Cloud WAN** generates an event when an **Amazon VPC** is attached into a segment. This event includes a JSON object that contains details such as 'attachment-id' and 'VPC-id.'
4. **Amazon EventBridge** captures this event. An **EventBridge** rule invokes a Regional **AWS Lambda** function.
5. **Lambda** accepts the event's JSON string as an input.
6. **Lambda** checks **Amazon VPC IP Address Manager** (IPAM) for a pool that has the same tag value as the **Amazon VPC** attachment, provided in step 2. In this example, the expected tag is Finance.
7. IPAM returns the Classless Inter-Domain Routing (CIDR) associated with the IPAM pool to **Lambda**.
8. **Lambda** adds a route to the **Amazon VPC** routing table with the CIDR that was obtained in step 7. The target for this route is the **AWS Cloud WAN** core network.
9. The same steps can be applied to **Amazon VPCs** in a different Region.
10. This completes the end-to-end routing for a multi-Region **AWS Cloud WAN** deployment

Reviewed for technical accuracy May 11, 2023

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture