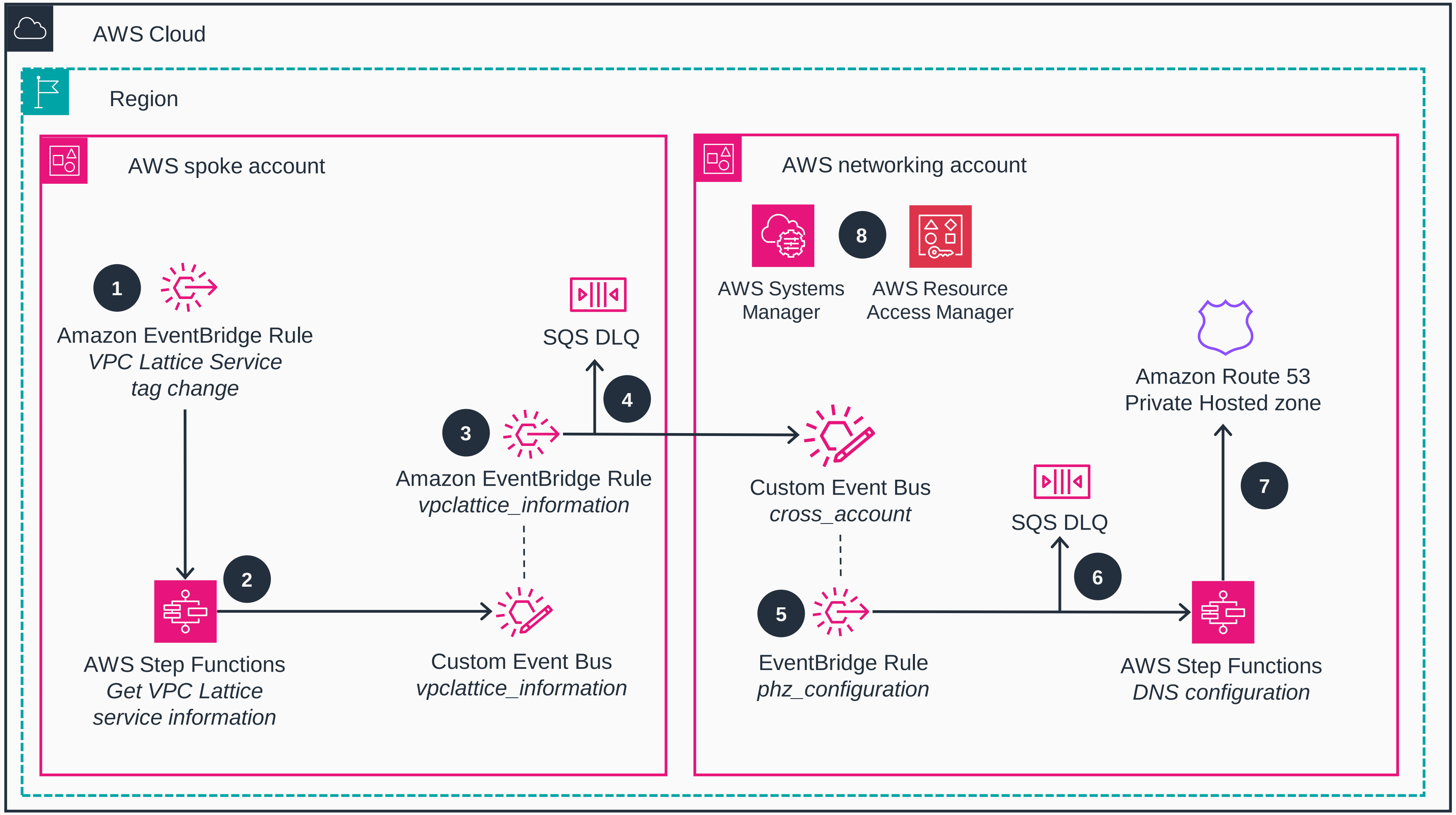
Guidance for Amazon VPC Lattice Automated DNS Configuration on AWS

This architecture diagram shows the automation of a DNS resolution configuration when creating new Amazon VPC Lattice services.



1. When a new spoke account creates a new **Amazon VPC Lattice** service, an **Amazon EventBridge** rule checks that a **VPC Lattice** service has been created with the proper tag. The **EventBridge** rule (default event bus) also verifies whether a **VPC Lattice** service has been deleted upon the removal of such tag.

2. The event is forwarded to the '*Get VPC Lattice service information*' **AWS Step Functions** state machine. Depending on the action (creation or deletion), the state machine publishes an event to the custom event bus. Additionally, for created resources with custom domain names, the state machine retrieves the domain name configuration details, including the domain name generated by **VPC Lattice**, the hosted zone managed by **VPC Lattice**, and the custom domain name.

3. The '*vpclattice_information*' custom event bus in the spoke account is configured with a target pointing to the '*cross_account*' event bus in the networking account.

4. Unsuccessfully processed events from delivery are stored in the **Amazon Simple Queue Service (Amazon SQS)** dead-letter-queue (DLQ) within the spoke account for monitoring.

5. The '*cross_account*' custom event bus in the networking account invokes the `*DNS configuration*` **Step Functions** state machine. This processes the notification sent from the spoke account.

6. Unsuccessfully processed events are stored in the DLQ in the networking account for monitoring.

7. The `*DNS configuration*` state machine creates or deletes the corresponding alias record in the private hosted zone.

8. **AWS Systems Manager** and **AWS Resource Access Manager (AWS RAM)** are used for secure parameter storage and cross-account data sharing.

Reviewed for technical accuracy January 24, 2025

AWS Reference Architecture