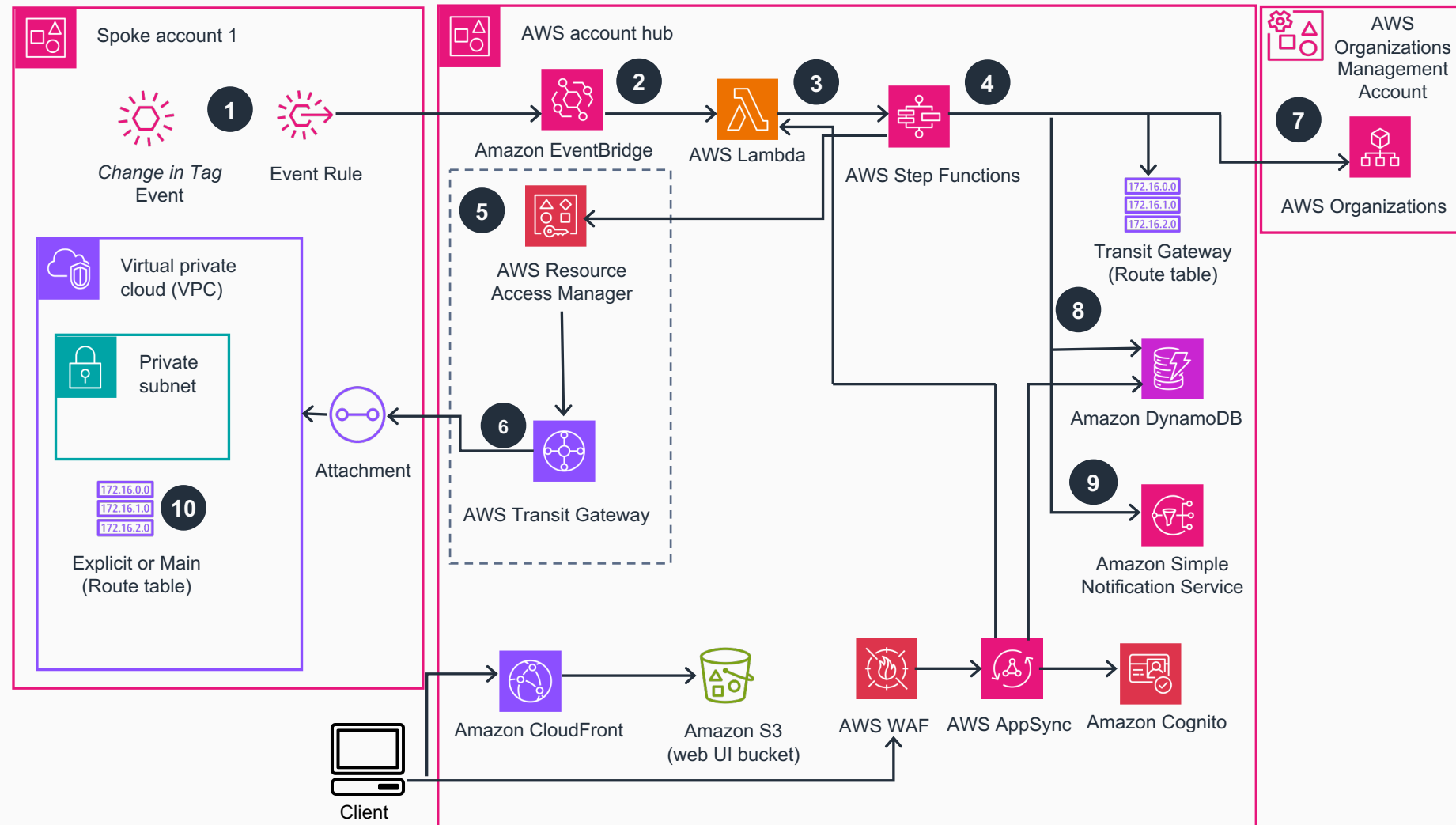


Guidance for Network Orchestration for AWS Transit Gateway

This architecture diagram illustrates how Network Orchestration for AWS Transit Gateway works. It shows the key components and their interactions, providing an overview of the architecture's structure and functionality.



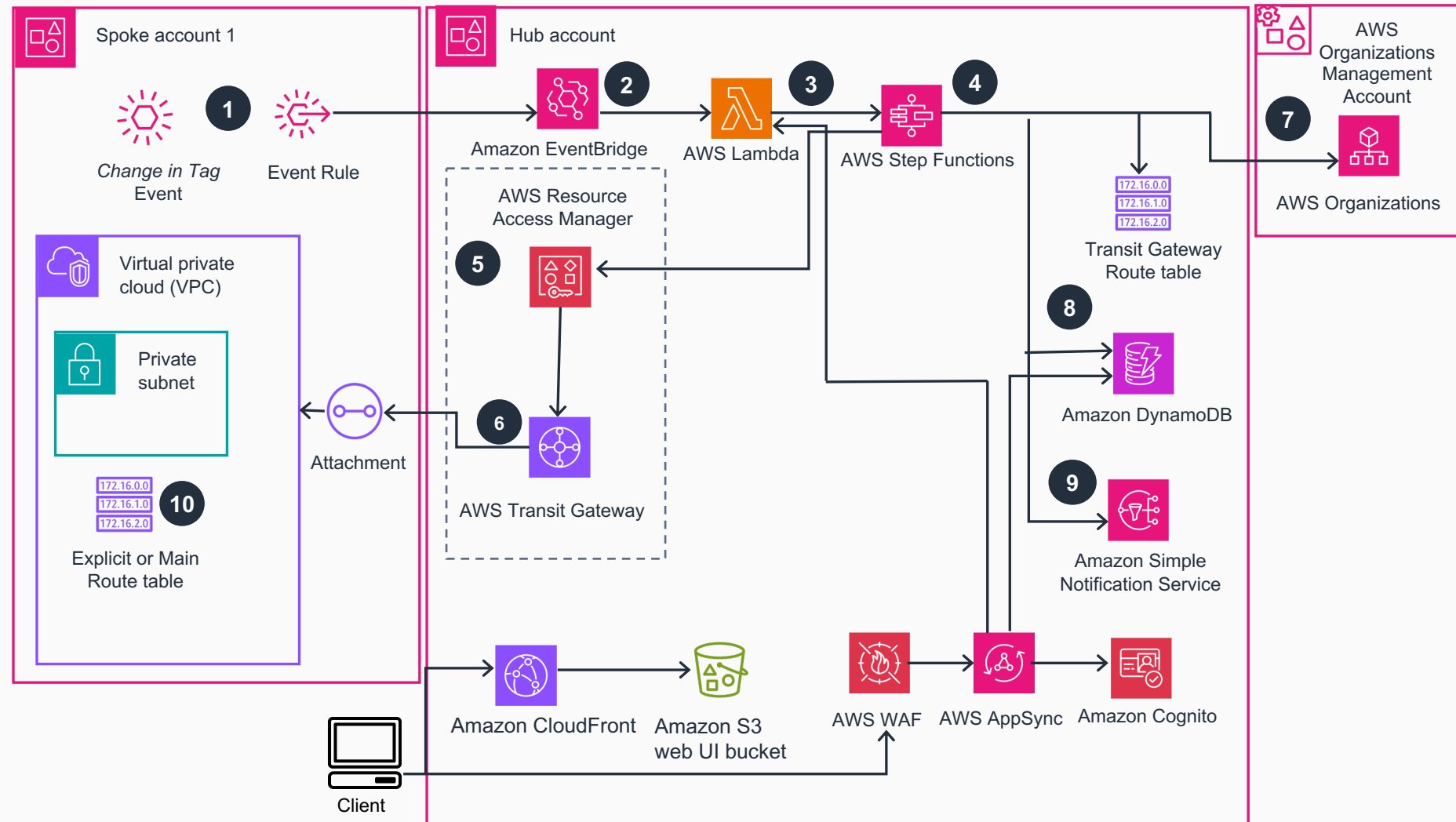
Reviewed for technical accuracy August 28, 2026
© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

1. An administrator tags a subnet with Attach-to-TGW (to create a TGW attachment and add routes to subnet route table) and/or the VPC with Associate-with / Propagate-to (to configure TGW route table association and propagation). **Amazon EventBridge** in the spoke account captures the tag-change event and forwards it to the hub accounts' EventBridge Bus.
2. **Amazon EventBridge** (in the hub account) receives the cross-account event and triggers the orchestration workflow.
3. **AWS Lambda** processes the event and initiates the **AWS Step Functions** state machine.
4. **AWS Step Functions** orchestrates the multi-step attachment workflow:
 - a. Retrieve account metadata (name, OU path) from **AWS Organization** for approval requiring routing decisions.
 - b. Create or validate the **Transit Gateway** VPC attachment via the shared TGW resource (shared through **AWS Resource Access Manager (RAM)**).
 - c. Associate the attachment with the TGW **Route table** specified in the Associate-with tag, and enables route table propagation specified in the Propagate-to tag
 - d. Updates the **VPC route table** in the spoke account with routes pointing to the TGW attachment.
5. **AWS Resource Access Manager (RAM)** shares the **Transit Gateway** from hub account to the spoke account, enabling cross-account attachment.
6. **AWS Transit Gateway** in the hub account processes the attachment request and associates it with/propagates to the designated route table
7. **AWS Organizations** is queried to retrieve account name and OU path. This information drives conditional approval rules (auto-approve / reject / require-approval based on OU membership) and is applied as tags to the TGW attachment for identification.
8. **Amazon DynamoDB** stores the state of all attachments, and workflow execution history.

Guidance for Network Orchestration for AWS Transit Gateway

This architecture diagram illustrates how Network Orchestration for AWS Transit Gateway works. It shows the key components and their interactions, providing an overview of the architecture's structure and functionality.



9. **Amazon Simple Notification Service (SNS)** sends notifications to administrators about the attachment status (success/failure/approval required).
10. The **VPC route table** in the spoke account is updated with routes directing traffic through the **Transit Gateway** attachment.

