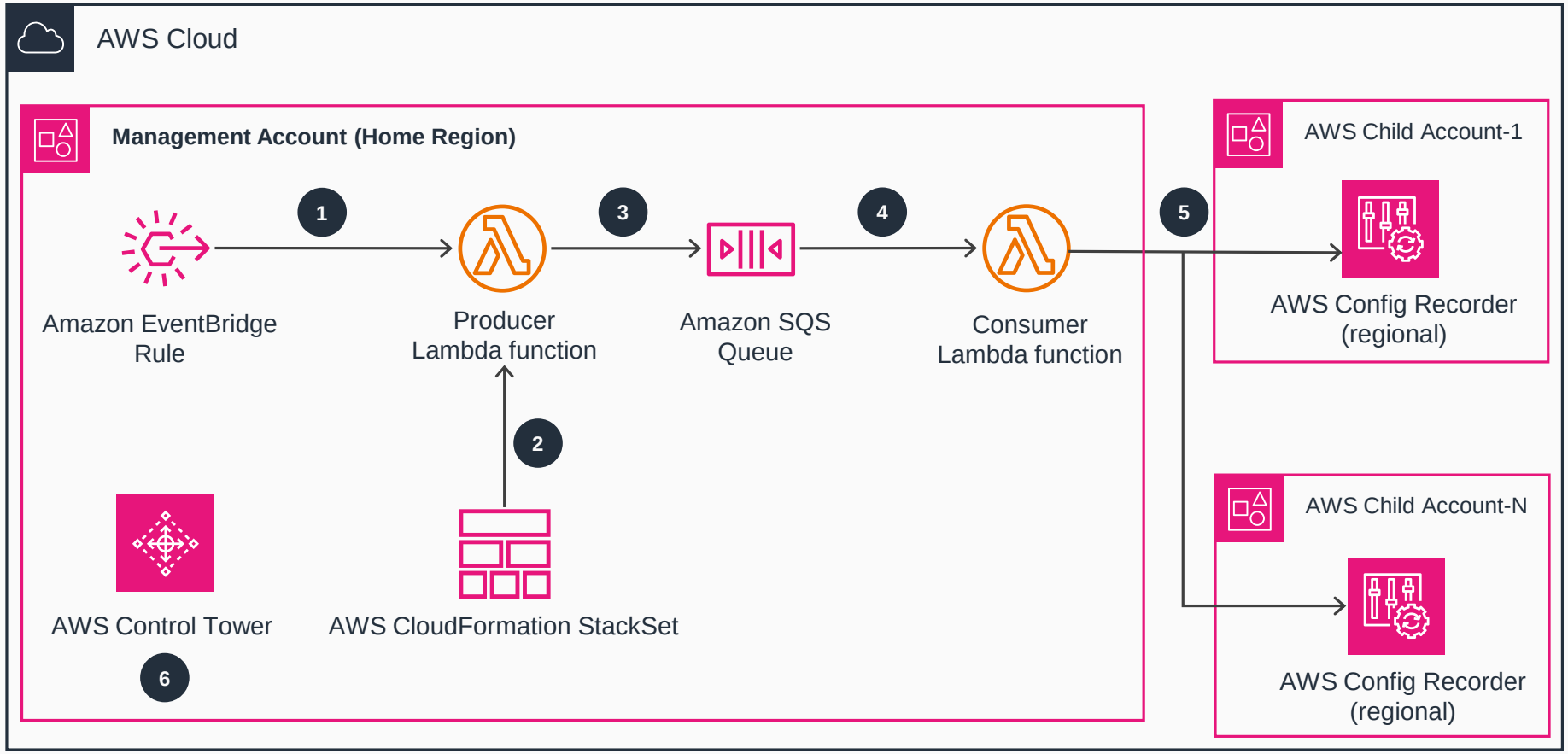
Guidance for Customizing AWS Config Resources in AWS Control Tower

The architecture diagram helps you to turn off recording in AWS Config for non-critical resources to keep AWS Config costs under control. Following the steps in this Guidance, you can make changes to AWS Config within the AWS Control Tower environment, without causing any drift in the landing zone.



1. An **Amazon EventBridge** rule invokes a producer **AWS Lambda** function when an **AWS Control Tower** account lifecycle event occurs.
2. The producer **Lambda** function queries the **AWS CloudFormation StackSet** responsible for deploying **AWS Config** recorder to collect all AWS Region and child account details.
3. The producer **Lambda** function identifies the list of accounts and Regions where the **AWS Config** recorder is enabled and generates individual messages for each account and Region in an **Amazon Simple Queue Service (Amazon SQS)** queue.
4. Every message in the **Amazon SQS** queue invokes a consumer **Lambda** function.
5. The consumer **Lambda** function assumes the AWSControlTowerExecution role in the member account and updates the **AWS Config** recorder with the resource list, specified as an input parameter, while deploying the Guidance.
6. You can continue to use **AWS Control Tower** to manage the AWS accounts without having to make any changes to the **AWS Config** resource tracking.

Reviewed for technical accuracy January 24, 2024

AWS Reference Architecture