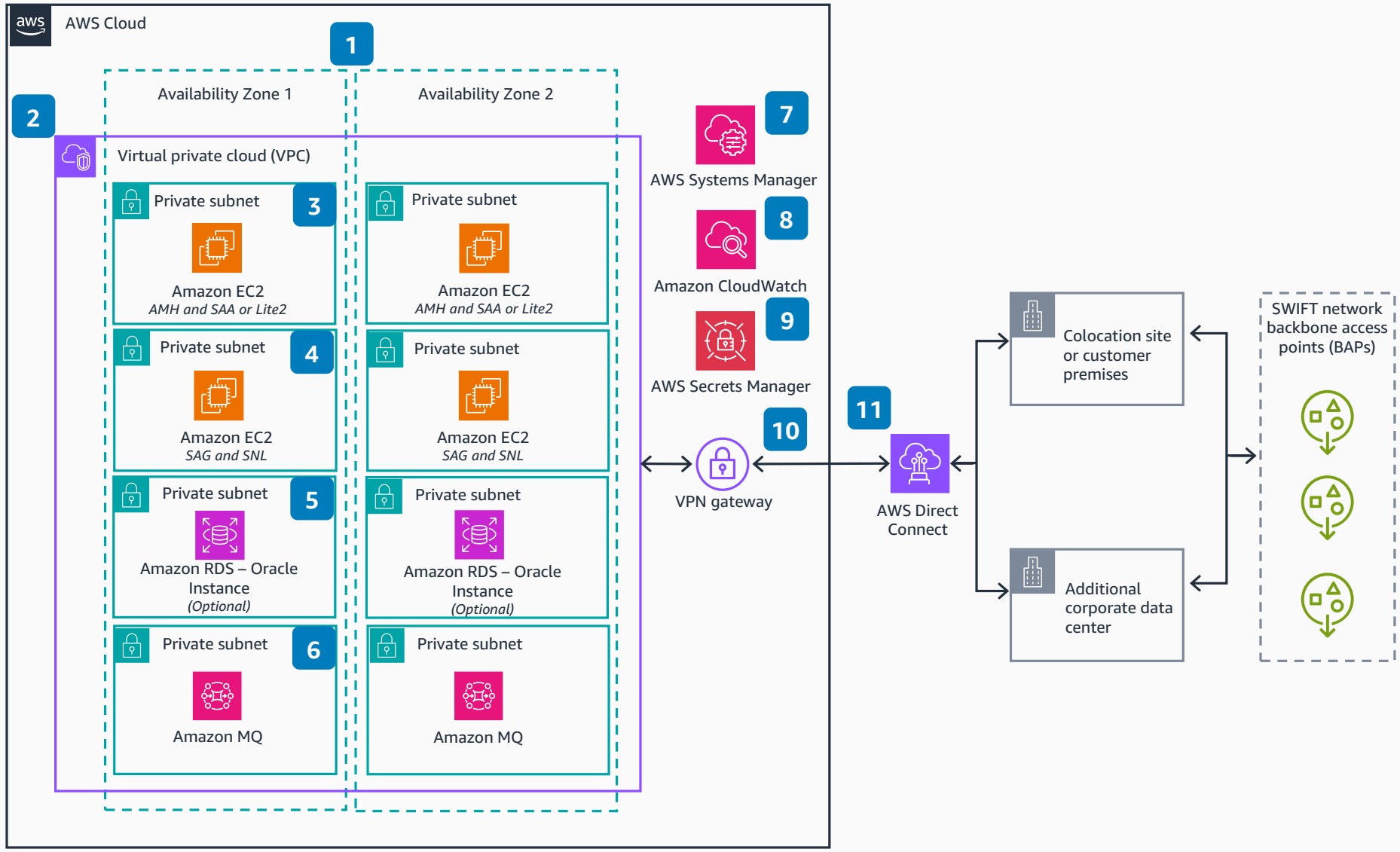
Guidance for Architecting SWIFT Connectivity on AWS

A standardized environment for connecting to the SWIFT network.



1. This architecture spans two Availability Zones.
2. **Amazon Virtual Private Cloud** (Amazon VPC) is configured with private subnets according to AWS best practices and follows the SWIFT Customer Security Programme (CSP).
3. An **Amazon Elastic Compute Cloud** (Amazon EC2) instance runs Alliance Messaging Hub (AMH) and SWIFT Alliance Access (SAA) or Lite2.
4. An **Amazon EC2** instance runs SWIFT Alliance Gateway (SAG) and SWIFTNet Link (SNL).
5. (Optional) An **Amazon Relational Database Service** (Amazon RDS) Oracle instance runs in active or standby mode to store configuration and message data for AMH.
6. An **Amazon MQ** instance manages communication for AMH.
7. **AWS Systems Manager** removes the need for a jump server.
8. **Amazon CloudWatch** provides the mechanism to store, access, and monitor SWIFT activities.
9. **AWS Secrets Manager** encrypts, stores, and retrieves passwords.
10. An **Amazon Virtual Private Network** (VPN) gateway with **Elastic Load Balancing** (ELB) connects the **Amazon VPC** to **AWS Direct Connect**.*
11. **Direct Connect** establishes private connectivity between AWS and data centers or colocation environments.*

*The AWS Cloud Development Kit (CDK) that deploys this Guidance does not include these components because they require design decisions on how to connect to the SWIFT network.

Reviewed for technical accuracy May 24, 2023

AWS Reference Architecture