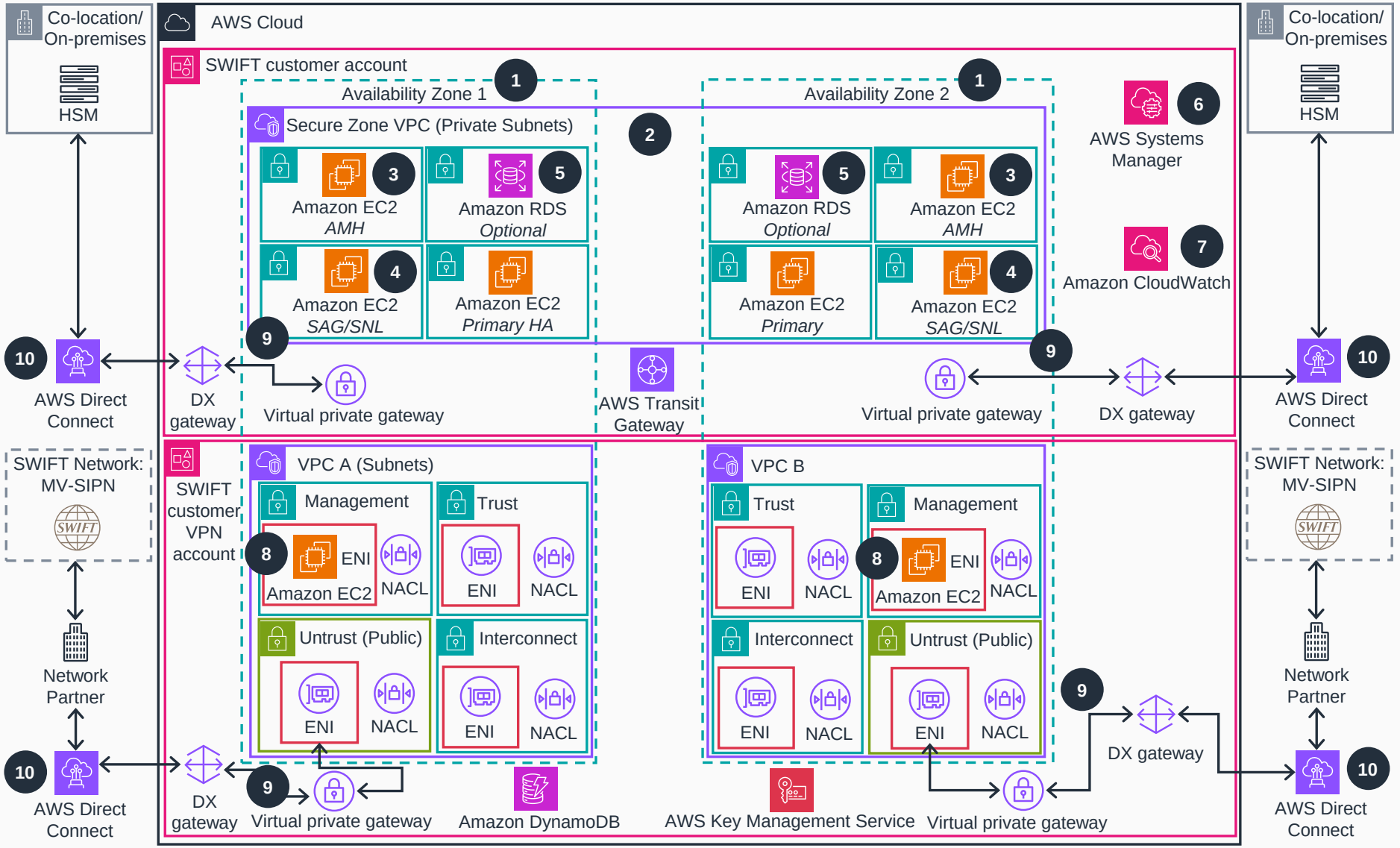
Guidance for SWIFT Alliance Connect Virtual on AWS

This architecture diagram shows a standardized environment for connecting to the SWIFT network.



1. Deploy the architecture to span two Availability Zones (AZs).
2. Configure an **Amazon Virtual Private Cloud (Amazon VPC)** with private subnets according to AWS best practices and following SWIFT's Customer Security Program (CSP) guidance.
3. An **Amazon Elastic Compute Cloud (Amazon EC2)** instance runs Alliance Messaging Hub (AMH) and SWIFT Alliance Access (SAA) or Lite2.
4. An **EC2** instance runs SWIFT Alliance Gateway (SAG) and SWIFTNet Link (SNL).
5. Optionally, an **Amazon Relational Database Service (Amazon RDS)** Oracle instance runs in active or standby mode to store configuration and message data for AMH.
6. **AWS Systems Manager** removes the need for a jump server.
7. **Amazon CloudWatch** provides the mechanism to store, access, and monitor logs and metrics of the SWIFT environment.
8. A Dual Alliance Connect Virtual **EC2** instance, based on Juniper vSRX platform, provides **AWS Virtual Private Network (AWS VPN)** connectivity to the SWIFT network.
9. An **AWS VPN** gateway connects the **Amazon VPC** to **AWS Direct Connect**.
10. **AWS Direct Connect** establishes private connectivity between AWS and data centers or colocation environments through a **Direct Connect (DX)** gateway.

Reviewed for technical accuracy July 29, 2024

AWS Reference Architecture