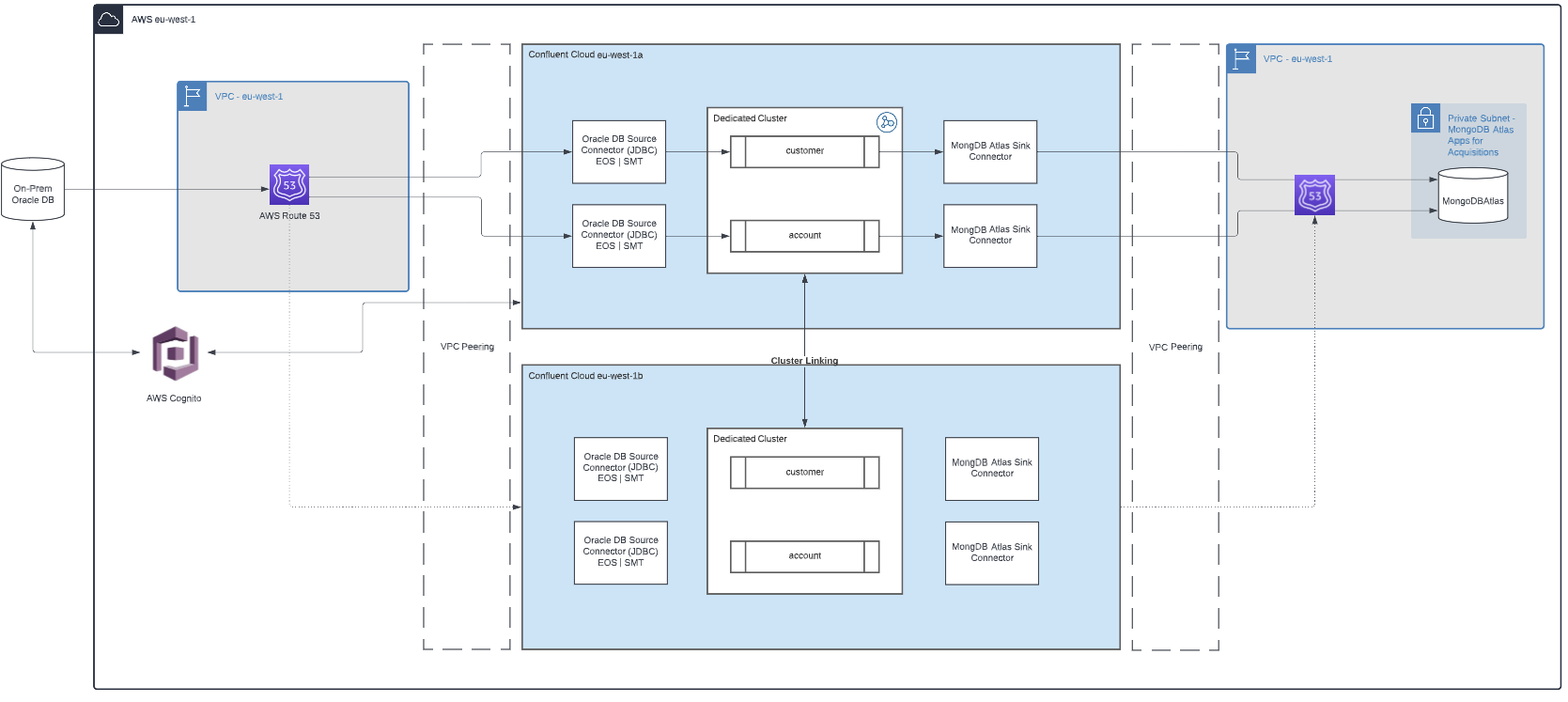
Dillon Carlson

Use Case 2 “A Bank Offloading”

GKO Pre-Work

### Future State Architecture



### Security Framework

Securing the environment will be handled in the control plane with SAs and RBAC to control provisioning and access to Confluent Cloud topics and clusters. AWS Cognito will be the Oauth2 provider. If this configuration isn’t necessary and the Bank already has Azure AD, then we can use that. Organization admin will be given to their highest ranked security personnel. CloudClusterAdmin and EnvironmentAdmin will be given to their leaders and closest engineers. Then NetworkAdmin will be given to their networking engineers. DeveloperManage will be given to developer leads. DeveloperWrite will be given to their developers on a per topic or cluster basis. DeveloperRead will be given to analysts or anyone who has a proper right and need to see the data. Other roles like MetricsViewer and ResourceOwner will be granted to personnel as the bank sees fit.

### Network Framework

The Confluent Cloud primary cluster will be hosted in AWS eu-west-1a and the cluster linked secondary cluster will be in eu-west-1b. There will be an active-passive architecture with the secondary cluster set up with connectors and topics on being mirrored from the primary cluster. The on-prem database will connect to the CC connectors via a Route53 gateway sitting inside of an AWS VPC in eu-west-1. The eu-west-1 VPC will connected to Confluent Cloud clusters via VPC Peering. Route 53 in the AWS VPC will be used for DR efforts. Route 53 will forward data coming from the on-prem Oracle DB in case of CC failure or failing a health check. Egress data connections will be VPC Peered to another VPC hosting the MongoDB Atlas instance. The VPC with MongoDB Atlas will have Route 53 take care of DR failover.

### Observability Framework

The Bank will use Datadog since they want to have a quick and easily integrated monitoring platform. The operations teams will develop metrics and alerts to be sent when there are under replicated ISRs and latencies outside their SLAs. If there is a failover or a health check failer from Route 53, all of operations, networking, and security will be alerted for an all hands bridge call to make sure data is flowing correctly in the anticipated path.