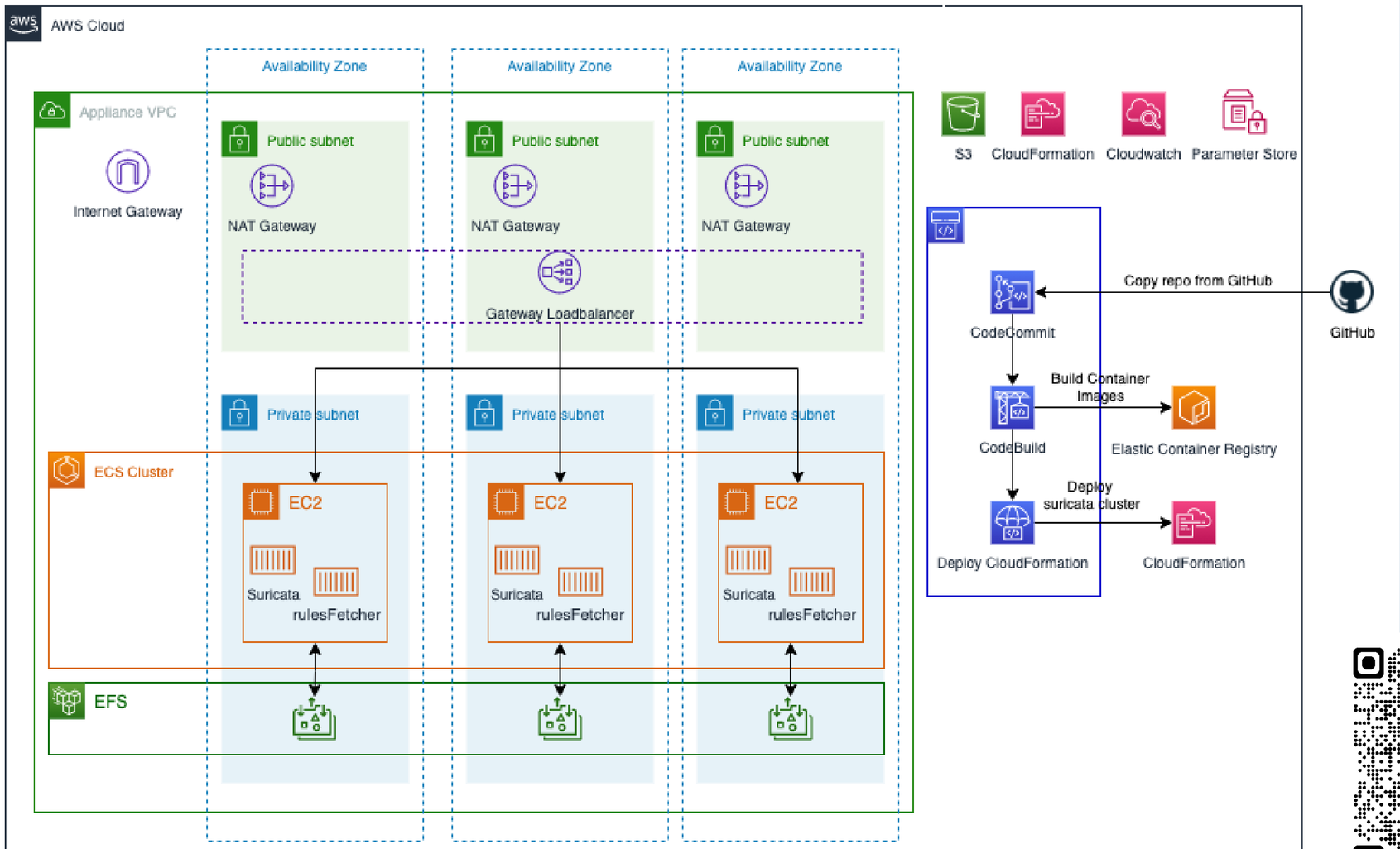
Building an Open Source IDS/IPS service on AWS with Suricata

Using Gateway Load Balancer

Adam Palmer
Jesper Eneberg
Nick Coval

Amazon Web Services

This solution deploys an open-source IDS/IPS service running in Docker containers, using Amazon Elastic Container Service (ECS) and Amazon Linux 2 (AL2). This service provides stateless packet inspection and logging, whilst leveraging the simplicity, elasticity and scalability enabled by Gateway Load Balancer (GWLB).



Project highlights:

- In-line Suricata IDS/IPS for distributed or centralized deployment models
- Open source
- Scalable with Gateway Load Balancer
- Customizable, extensible and portable
- Leverages AWS native services
- GitOPS driven
- Supports GeoIP referencing and Lua logging and scripting

<- Blog link for step-by-step guide and code samples

Learn more at our SuriCon session on Thurs 10/21 @ 10:15 AM ET

SURICON BOSTON 2021

OISF

Adam Palmer (adampalm@amazon.com) / Jesper Eneberg (enebergj@amazon.com) / Nick Coval (nickaws@amazon.com)