Protecting Compute Resources

Securing Amazon EC2 Instances

The process for securing EC2 instances involves principles that are applicable to any OS, whether running in a virtual machine or on premises:

- **Least Access:** Restrict server access from both the network and on the instance, install only the required OS components and applications, and leverage host-based protection software.
- **Least Privilege:** Define the minimum set of privileges each server needs in order to perform its function.
- **Configuration Management:** Create a baseline server configuration and track each server as a configuration item. Assess each server against the current recorded baseline to identify and flag any deviations. Ensure each server is configured to generate and securely store appropriate log and audit data.
- **Change Management:** Create processes to control changes to server configuration baselines.
- **Audit Logs:** Audit access and all changes to EC2 instances to verify server integrity to ensure only authorized changes are made.

For more information on securing EC2 instances please see: https://aws.amazon.com/answers/security/aws-securing-ec2-instances/

This white paper provides an overview of security when using Lambda: https://d1.awsstatic.com/whitepapers/Overview-AWS-Lambda-Security.pdf

Amazon Elastic Container Service (Amazon ECS)

Amazon ECS allows you to specify an IAM role for each ECS task. This allows the Amazon ECS container instances to have a minimal role, respecting the ‘least privilege’ access policy and allowing you to manage the instance role and the task role separately. You can also use Amazon CloudWatch Logs to gain visibility into the IAM role to which a task is assigned. More details on Amazon ECS can be found at: https://aws.amazon.com/ecs/features/