AWS EC2 Confidential Compute Options

Choosing the Right Protection for Your Workloads

Alexander Graf
Principal Engineer
Amazon Web Services

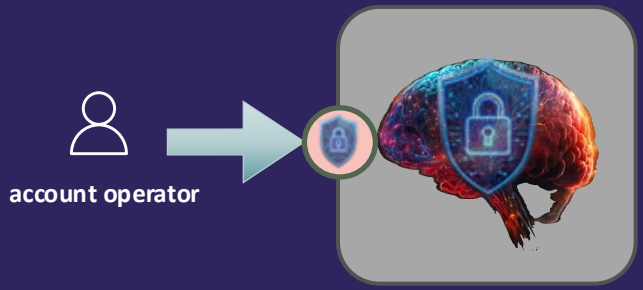
Confidential Computing

Confidential Computing

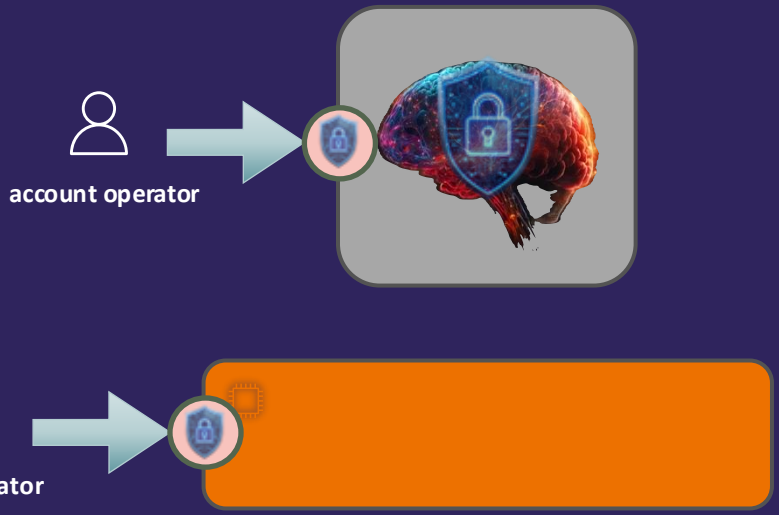
Confidential Computing

Confidential Computing

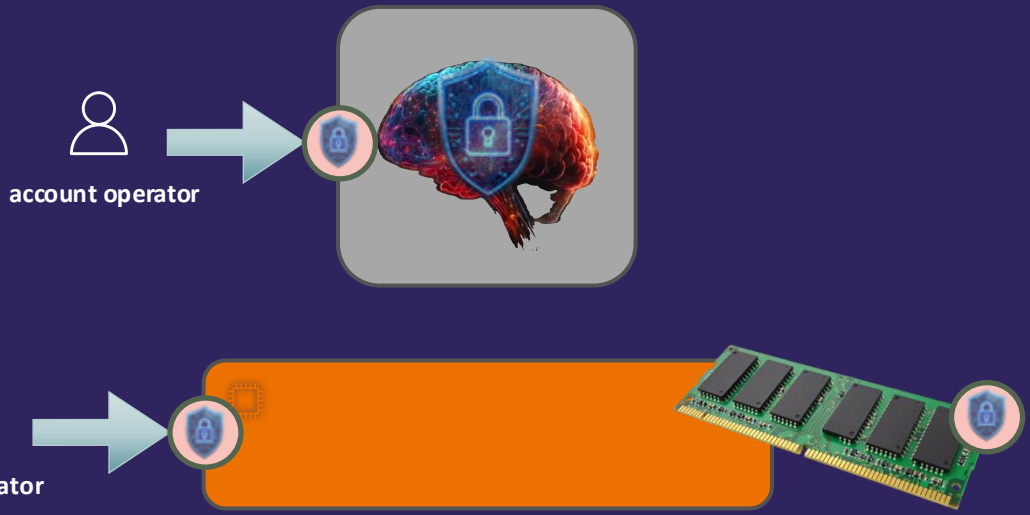
Confidential Computing



Confidential Computing

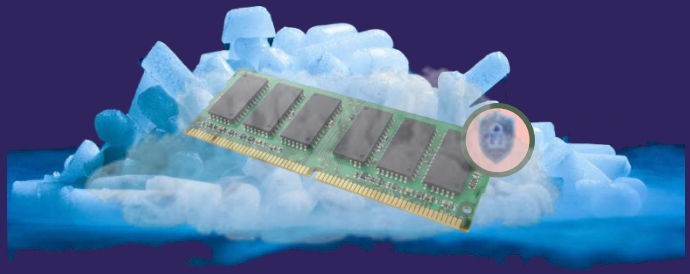


Confidential Computing

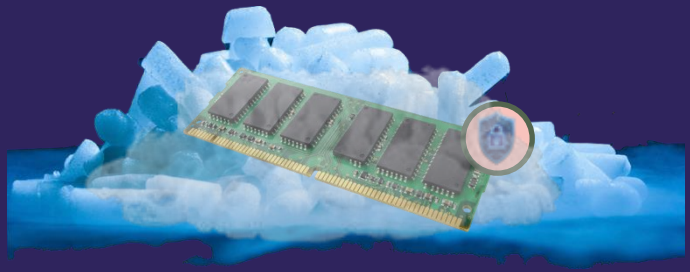


Memory Encryption

Memory Encryption



Memory Encryption



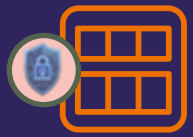
Memory Encryption

- Graviton2 or newer
- Intel Xeon 3rd gen or newer
- AMD EPYC 3rd gen or newer

Account Operator

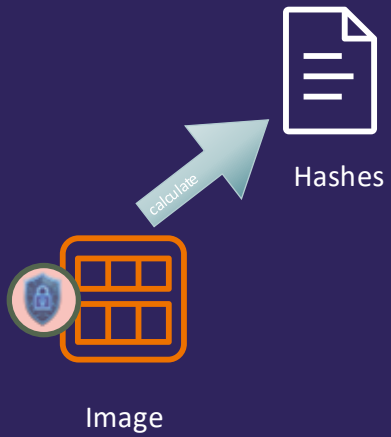
Image

Account Operator



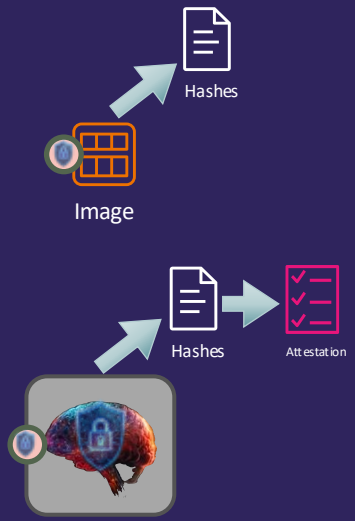
Image

Account Operator

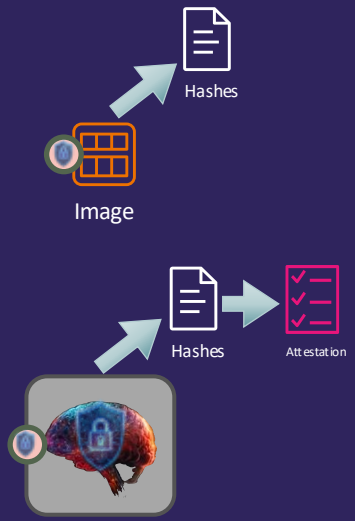


Account Operator

EC2 Instance Attestation

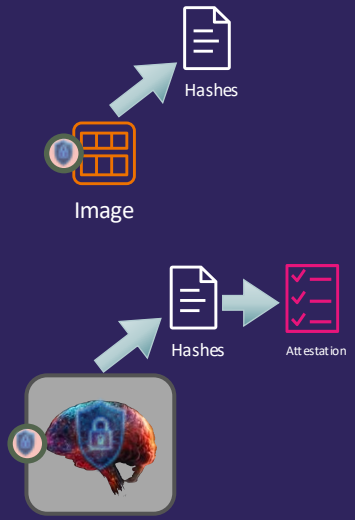


EC2 Instance Attestation



AL2023 & NixOS templates

EC2 Instance Attestation

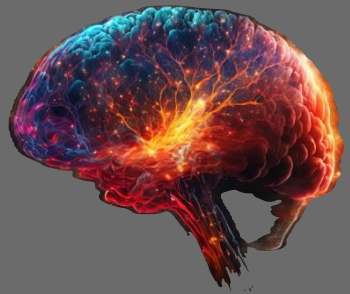


AL2023 & NixOS templates

NitroTPM Attestation Document

Nitro Enclaves

Nitro Enclaves

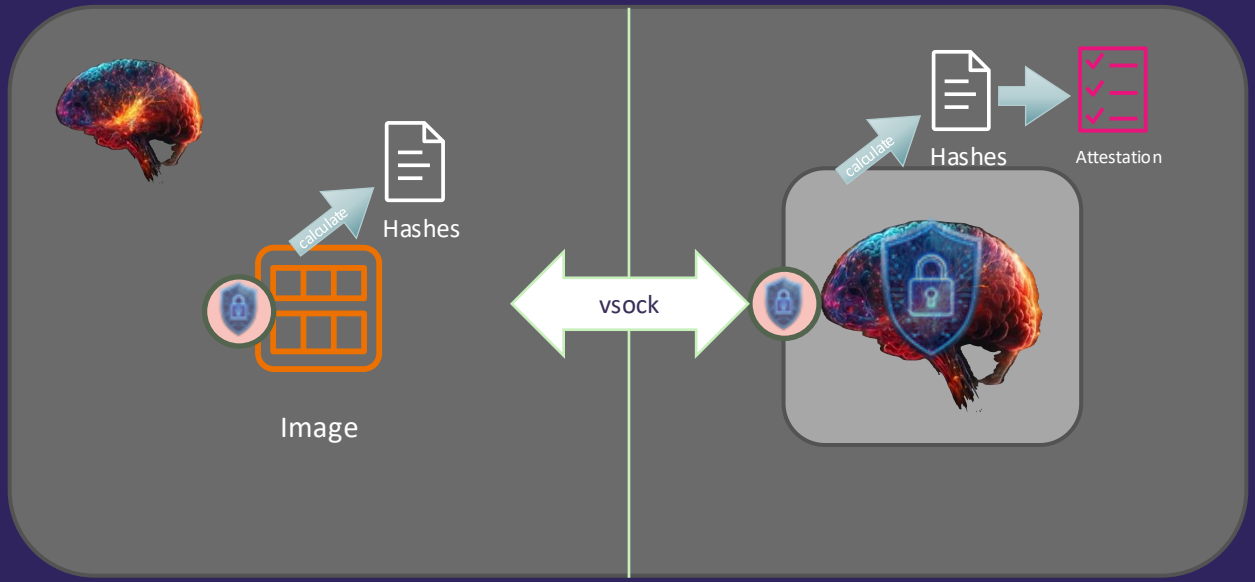


Nitro Enclaves

Nitro Enclaves

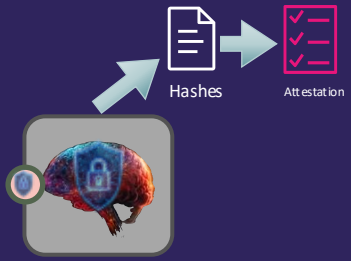
Nitro Enclaves

Nitro Enclaves



Nitro Enclaves

Convert container to EIF



Nitro Enclaves Attestation Document

KMS and Attestation

Image Hash

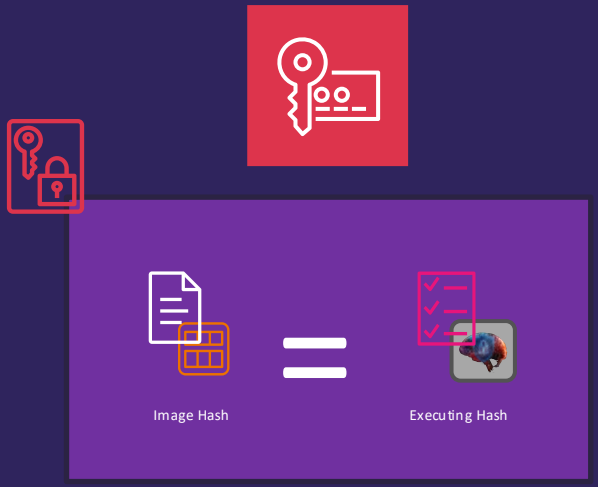
Executing Hash

KMS and Attestation

Image Hash

Executing Hash

KMS and Attestation



Confidential Computing

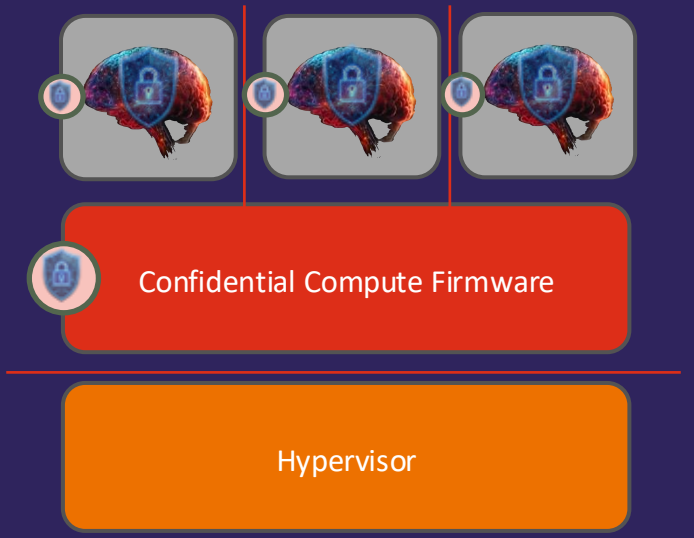
Hypervisor

Confidential Computing

Confidential Compute Firmware

Hypervisor

Confidential Computing

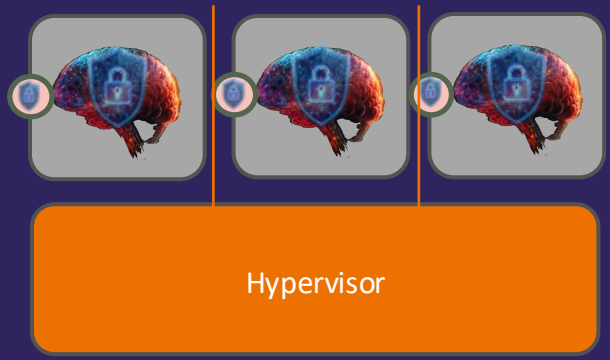


Confidential Computing

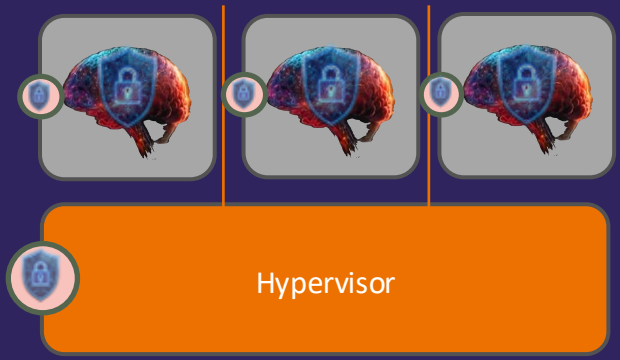
SEV-SNP Availability

- All bare metal AMD instances
- Virtualized on C/M/R 6a in eu-west-1 & us-east-2

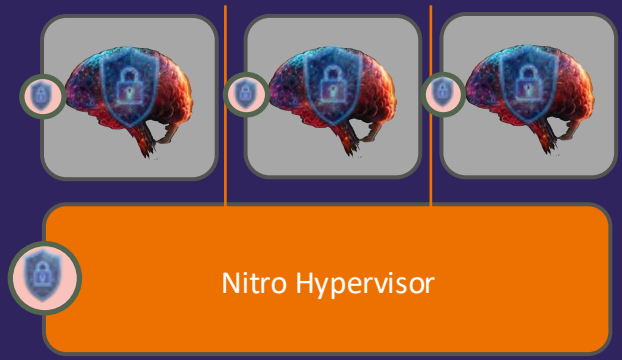
Confidential Computing



Confidential Computing



Confidential Computing



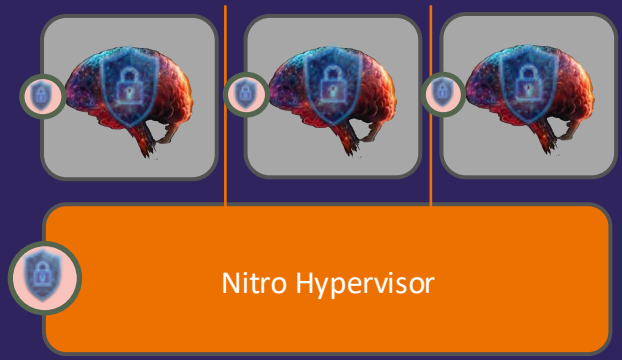
Confidential Computing

96. AWS Nitro System

AWS personnel do not have access to Your Content on AWS Nitro System EC2 instances. There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access Your Content on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance. Access to AWS Nitro System EC2 instance APIs – which enable AWS personnel to operate the system without access to Your Content - is always logged, and always requires authentication and authorization.

https://aws.amazon.com/service-terms/

Confidential Computing



Confidential Computing

Confidential Computing

Nitro Isolation Engine

- Graviton5 exclusive
- Formally verified TCB
- Double protection

AWS Confidential Computing

AWS Confidential Computing

Demystify attestation: Cryptographically verify execution environment

Introducing Nitro Isolation Engine: Transparency through Mathematics

Innovating with AWS Confidential Computing: An Integrated Approach

Thank you