# Assignment 2

Garrett Gruss 4976-3695

February 6, 2026

## Abstract

## 1 Introduction

EC2 is Amazon Web Services's (AWS) primeier service for scalable compute in the cloud. Launched in the beginning of 2018, AWS Nitro is a combination of purpose built server designs, data processors, system management components, and specialized firmware acting as the underlying platform that all EC2 instances run on.

## 2 Core Components

The core components of the AWS Nitro system consists of purpose-built Nitro cards, the Nitro security chip, and the Nitro hypervisor. Together, these components form the EC2 control plane

### 2.1 Nitro Cards

Each Nitro system is composed of multiple Nitro cards stacked within a Nitro Server. These cards share power and PCIe interfaces with a host Nitro

Controller. Each Nitro Card runs on purpose built hardware designed by Annapurna Labs, with firmware designed by dedicated AWS engineering teams.

## 2.2 Nitro Hypervisor

The Nitro hypervisor is responsible for managing the virtual machine (VM) of each EC2 instance running on the Nitro system. The hypervisor handles tasks such as resource isolation, control of privileged instructions, TBD. The hypervisor is designed with security first, and cannot initiate outbound communication or allow user access, as it does not have a shell or any general operating-system components.

The hypervisor guards against side-channel attacks by ensuring the CPU Threads and L1/L2 cache are never shared amongst EC2 instances.

## 2.3 Nitro Controller

The Nitro security chip is responsible for secure boot and operating of the Nitro system. It continuously Intercepts and moderates all operations to local firmware at runtime, and alarms on anomalous behavior. During boot, it securely unlocks the system to guard against TBD.

## 2.4 Specialized Nitro Cards

The Nitro system contains several specialized cards responsible for networking, block storage, and file storage. The Nitro VPC card contains physical I/O network interfaces which is virtualized and distributed to EC2 instances through TBD. Storage is handled through the Nitro EBS card for block storage, and the local NVMe card for file storage. The hypervisor is responsible for attaching storage from these cards to each EC2 instance.

# 3 Physical Security

AWS employs additional site security such as physical access control, and continuous security monitoring to ensure no unauthorized person enters the datacenter. All storage devices removed from the Nitro system are physically destroyed to ensure no data is leaked.

# 4 References

1. Amazon Web Services. "The Security Design of the AWS Nitro System." AWS Whitepaper, 2026. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html