Ejercicios Tema 1
Garantía y Seguridad UZ, 2025-26

Lacueva Sacristán, Héctor

05/02/2026

Índice

T1.1 Amazon Nitro **2**
Introducción . . . 2
Componentes del "Nitro System" . . . 2
Nitro Cards . . . 2
Nitro Security Chip . . . 2
Nitro Hypervisor . . . 2

Referencias **2**

T1.1 Amazon Nitro

Toda la información ha sido obtenida de las siguientes referencias (*Nitro* 2022) y (*The Security Design of the AWS Nitro System* 2024).

Introducción

El **"Nitro System"** es la base para las instancias modernas de Amazon EC2 (Elastic Compute Cloud). Se trata de un diseño que ofrece **gran seguridad**, **aislamiento**, **alto rendimiento** y **bajo coste** en servidores Cloud.

Previo a este sistema se empleaba un hipervisor de tipo 1 "típico", que operaba una distribución ligera de Linux en la que se gestionaban todos los recursos ofrecidos a las VM.

Componentes del "Nitro System"

Nitro Cards

Componentes hardware dedicados a la E/S con altas capacidades de procesado que operan al margen del servidor principal. Se conectan a través de PCIe.

La **Nitro Card** principal se denomina **Nitro Controller** y **es la base de la confianza del sistema** y se encarga de gestionar todos los componentes del servidor.

Nitro Security Chip

Actúa como un puente de seguridad que extiende la confianza del Nitro Controller al servidor y como un firewall que impide modificaciones no autorizadas del firmware.

Nitro Hypervisor

Se trata de un hipervisor de tipo 1 (Nativo) **muy ligero** (basado en KVM), enfocado en la seguridad, y que trabaja lo justo y necesario. Recibe comandos del Nitro Controller para particionar memoria y recursos de CPU utilizando el soporte de virtualización ofrecido por el procesador del servidor. El resto de funciones las **delega a las Nitro Cards**.

Además, se encarga de asignar los aceleradores de hardware disponibles a las VM y de la recuperación ante errores de hardware.

El contenido del hipervisor es tan mínimo que no cuenta con sistema de ficheros, apartado de red, soporte para periféricos, etc. Tampoco incluye acceso a través de una "shell" ni un modo de acceso iterativo lo que resulta en una mayor seguridad en comparación a otros hipervisores.

El código del hipervisor, es un componente de firmware firmado criptográficamente que está guardado en el almacenamiento local encriptado (un NVMe read-only) del Nitro Controller. Al configurarse el uso del hipervisor, se carga la copia segura desde el Nitro Controller al servidor.

El hecho de que el hipervisor delegue el procesado de datos y la virtualización de la E/S a las Nitro Cards **mejora el rendimiento** (prácticamente ***"bare metal"***) y la **seguridad** (isolation).

Al ser tan límitado el hipervisor erradica muchos bugs que se dan en otros hipervisores (remote networking attacks or escalada de privilegios a base de drivers) y crea un ambiente inhóspito para los atacantes.

Por último, también se debe destacar que la actualización del hipervisor es prácticamente instantánea y el cliente no se ve afectado por ello, mientras que en otros sistemas esto puede ser un problema.

Referencias

Nitro: Cómo El Sistema de Virtualización Soporta Las Nuevas Generaciones de Amazon EC2. 2022. https://www.youtube.com/watch?v=ZX0xzL2wgMc.

The Security Design of the AWS Nitro System. 2024. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html.