Ejercicios Tema 1
Garantía y Seguridad UZ, 2025-26

Lacueva Sacristán, Héctor

05/02/2026

Índice

T1.1 Amazon Nitro

La información ha sido obtenida de la siguiente referencia (*The Security Design of the AWS Nitro System* 2024). También hay un vídeo (*Nitro* 2022) que trata el tema.

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.

Componentes del "Nitro System"

El "Nitro System" funciona gracias a los siguientes componentes

- Nitro Cards
- Nitro Security Chip
- Nitro Hypervisor: aunque es **prescindible** si la instancia es **bare metal**.

Nitro Cards

Componente hardware dedicado 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** (**"Root of Trust"**) y se encarga de **gestionar todos los componentes del sistema nitro**.

Nitro Security Chip

Se trata de un chip dedicado a la seguridad del sistema. Actúa como un puente de seguridad entre las Nitro Cards y el servidor que extiende la confianza del Nitro Controller y, además, actúa 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[1]), **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**. Por otro lado, se encarga de asignar los aceleradores de hardware disponibles a las VM y de la recuperación ante errores de hardware.

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** frente a otros hipervisores (prácticamente ***"bare metal"***) y la **seguridad** (aislamiento).

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**. Al ser tan límitado, erradica muchos de los bugs y problemas que se dan en otros hipervisores (por ejemplo, ataques de red remotos) y crea un ambiente inhóspito para los atacantes.

El código del hipervisor, es un componente de firmware firmado criptográficamente que está guardado en el almacenamiento local seguro (un NVMe read-only) del Nitro Controller. Al configurarse el uso del hipervisor, se carga la copia segura desde el Nitro Controller al servidor y, gracias a esto, no puede sufrir modificaciones no autorizadas.

Por último, otra de las características del este hipervisor es que en caso de ser necesario actualizarlo, la afectación al usuario es ínfima.

[1] *"KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc."* (*Kernel Virtual Machine*, n.d.)

Referencias

Kernel Virtual Machine. n.d. https://www.linux-kvm.org/page/Main_Page.

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.