API de AWS Nitro System y declaraciones de seguridad

Amazon Web Services, Inc.
Versión 1.0 — 11 de abril de 2023

Preparado por
John Redford
Xiang Wen Kuan

Preparado para
Amazon Web Services

1 Resumen ejecutivo

Sinopsis

En el último trimestre natural de 2022, Amazon Web Services (AWS) contrató a NCC Group para que llevara a cabo una revisión de la arquitectura del diseño de AWS Nitro System, con especial atención a las declaraciones específicas de AWS en relación con la seguridad de las API del sistema Nitro. La planificación y ejecución de este trabajo continuaron durante el primer trimestre natural de 2023.

A continuación, se incluye una breve descripción del sistema Nitro, elaborada a partir de la documentación pública[1]:

> AWS Nitro System es una combinación de diseños personalizados de servidores, procesadores de datos, componentes de administración de sistemas y firmware especializado que proporcionan la plataforma subyacente para todas las instancias de Amazon EC2 lanzadas desde principios de 2018. Los tres componentes clave del sistema Nitro son estos:
>
> - Tarjetas Nitro personalizadas: dispositivos de hardware diseñados por AWS que proporcionan un control general del sistema y una virtualización de entrada/salida (E/S) independiente de la placa del sistema principal, con sus CPU y su memoria.
> - Chip de seguridad Nitro: facilita un proceso de arranque seguro para todo el sistema basado en una raíz de confianza del hardware, la capacidad de ofrecer instancias bare metal y una defensa en profundidad que ofrece protección al servidor frente a la modificación no autorizada del firmware del sistema.
> - Hipervisor Nitro: un hipervisor similar a un firmware, minimizado deliberadamente, diseñado para proporcionar un sólido aislamiento de los recursos y un rendimiento casi indistinguibles de los de un servidor bare metal.

AWS presenta una serie de declaraciones de seguridad respecto a cómo el sistema Nitro está diseñado para evitar que los empleados de AWS accedan a los datos de los clientes. Las declaraciones se enumeran en la parte correspondiente a las Declaraciones de este informe.

El sistema Nitro se ha diseñado para satisfacer los objetivos de seguridad que cubren estas declaraciones al proporcionar una infraestructura total de administración, gestión y supervisión de sistemas que opera desde el nivel de hardware hasta el aprovisionamiento y el despliegue y el final de la vida útil de los sistemas. AWS no tiene rutas de acceso secundarias o alternativas a los sistemas host de EC2 de Nitro. Este grado de rigurosidad y la adecuada alineación de los objetivos de seguridad con las prácticas empresariales sostenibles y alcanzables permitieron a AWS diseñar un sistema que respaldara unas declaraciones muy firmes de los clientes respecto a la seguridad y la privacidad.

Desde el punto de vista del diseño, NCC Group no detectó brechas en el sistema Nitro que pudieran poner en entredicho estas declaraciones de seguridad. Todos los diseños implican ventajas y desventajas, y AWS ha elegido un diseño en el que el impacto de un ataque malintencionado sería similar al de un fallo de hardware a pequeña escala.

Logística del proyecto

El alcance del análisis abarcó la verificación de una serie de declaraciones de seguridad relacionadas con el diseño de las API administrativas de Nitro, así como los procesos administrativos y de desarrollo que crean y administran las API de Nitro. Los operadores de AWS utilizan las API de Nitro para realizar un conjunto de tareas bien definidas que abarcan el desarrollo y el despliegue de los elementos de software del sistema Nitro, la infraestructura que utiliza y los procedimientos para crear y desplegar un entorno del sistema Nitro.

1. El diseño de seguridad de AWS Nitro System. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html.

El alcance de la evaluación de NCC Group abarcaba lo siguiente:

- La API del sistema Nitro, sus solicitudes, funcionalidad, procesos de desarrollo y despliegue y los elementos de infraestructura de apoyo que requiere.
- La función de los operadores de AWS que tienen acceso autorizado a las API del sistema Nitro.
- Los empleados de AWS que no son operadores, incluidos los desarrolladores del sistema Nitro y el personal que administra y asigna funciones a los empleados.
- Una revisión adecuada del sistema Nitro y su entorno para garantizar que no haya sistemas alternativos presentes o necesarios por diseño.

Los siguientes elementos no estaban incluidos en el alcance:

- Evaluación de los servicios del plano de control de EC2 en general.
- Evaluación del hipervisor Nitro, el firmware Nitro y el software Nitro de las tarjetas Nitro.
- Evaluación de las tarjetas Nitro.
- Evaluación del entorno físico y de los controles de seguridad física.

Metodología de evaluación

La evaluación se llevó a cabo en gran medida mediante entrevistas con el equipo de desarrollo de AWS Nitro y mediante el acceso a la documentación proporcionada por AWS. NCC Group entrevistó a varios ingenieros distinguidos del equipo de Nitro, incluido el ingeniero principal. Estas entrevistas cubrieron el origen y los objetivos de diseño del sistema, así como sus características y limitaciones operativas. Además, se proporcionó información en documentos y a través de pantallas compartidas para que NCC Group pudiera comprender a fondo la seguridad del Sistema Nitro. La documentación proporcionada abarcó numerosos detalles internos del diseño.

La evaluación no incluye una revisión en profundidad de la implementación de componentes concretos ni ninguna prueba práctica o validación técnica. La evaluación de las declaraciones se basó en el grado en que el diseño del Sistema Nitro, tal como se evaluó y observó, proporcionaba los medios para respaldar estas declaraciones y garantizar su mantenimiento. Como se trataba de una revisión a nivel de diseño, cualquier incumplimiento de este objetivo en el propio diseño tendría como resultado que no se considerase que una declaración estaba respaldada.

Limitaciones del proyecto

Esta actividad representa una evaluación puntual de las API de sistema Nitro. Las amenazas a la seguridad y las técnicas de los atacantes evolucionan rápidamente, y los resultados de esta evaluación no implican la aprobación de la idoneidad de las medidas de seguridad actuales contra las amenazas futuras. Además, las afirmaciones de NCC Group hacen referencia al sistema tal como se presentó durante el período de evaluación y no ofrecen ninguna garantía con respecto a cambios técnicos o desviaciones futuras elegidos u obligados en la política. Si bien el proceso de arranque seguro y la interacción de las tarjetas Nitro fueron un factor del análisis, la seguridad de estos sistemas en presencia de un atacante físico se aplazó a ese otro trabajo o se excluyó del alcance.

Esta revisión se basa en los testimonios del personal de AWS y en los documentos de diseño del producto presentados a NCC Group. Si bien AWS proporcionó el apoyo adecuado en ese sentido, NCC Group no puede dar fe de la precisión de la información o las conclusiones asociadas, ni de si la implementación coincide con el diseño. Todas las afirmaciones sobre lo que hace el sistema Nitro hacen referencia a su diseño.

2 Diseño del sistema Nitro

Introducción

NCC Group llevó a cabo una revisión del diseño arquitectónico del sistema Nitro que incluyó varias semanas de debates y análisis, con una planificación y revisión adicionales a lo largo de varios meses. El objetivo de la revisión era determinar si la arquitectura del sistema Nitro satisfacía las declaraciones de seguridad de AWS. El equipo de consultoría consideró el sistema desde la perspectiva de los «operadores de AWS», personas con acceso no público al entorno, así como de los desarrolladores del sistema Nitro y otros empleados de AWS.

El análisis también determinó que estas API son el único medio que tienen los operadores de AWS para interactuar con los hosts de instancias y que no hay otras formas de conectarse, iniciar sesión u obtener ningún otro tipo de acceso privilegiado. El análisis también determinó que ningún otro empleado de AWS, aparte de los operadores de AWS, puede utilizar estas API.

Objetivos de diseño del sistema Nitro

Privilegio mínimo

El diseño del sistema Nitro se adhiere al principio de privilegio mínimo. El diseño incluye la prohibición de:

- Acceder a los datos de los clientes.
- Acceder para ejecutar comandos o códigos arbitrarios.
- Personalizar una instancia con versiones de software o parches únicos.
- Migrar o almacenar datos en otra instancia o entorno.
- Realizar actividades no registradas.
- Realizar procedimientos de emergencia para eludir o eliminar las protecciones de seguridad.

El diseño del sistema Nitro se adapta a los requisitos esenciales de los entornos para gestionar eventos de pérdida de disponibilidad a pequeña escala, como fallos de hardware convencionales o un accidente. El alcance del posible abuso por parte de un usuario malicioso tendría un impacto similar al de esos eventos.

Redundancia y confianza cero

Los componentes del sistema Nitro están diseñados para realizar controles de seguridad redundantes y en capas. El diseño garantiza que la autenticación y la autorización se comprueben varias veces y que se requieran varias rutas para desarrollar e implementar los cambios de software. Los hosts de instancias están diseñados para verificar de forma independiente los controles de acceso adecuados antes de realizar cualquier acción solicitada.

Confidencialidad e integridad

En todo el diseño del entorno hay controles sólidos de cifrado y firma. El diseño general del sistema Nitro incluye garantizar que todas las comunicaciones del sistema Nitro estén cifradas de forma segura y que todos los componentes del sistema Nitro desplegados estén firmados y validados. Para reducir la probabilidad de poner en peligro las claves que protegen las comunicaciones y las actualizaciones de software, el diseño garantiza que las raíces de confianza se encuentren en sistemas seguros que no dependen de niveles más bajos de control de acceso para la gestión de la seguridad.

Auditoría y supervisión

Todas las solicitudes de la API del sistema Nitro se registran en un entorno seguro de CloudWatch con controles de acceso por capas. Los registros se supervisan constantemente para detectar el uso de solicitudes confidenciales o patrones de actividad que llamen la atención de las personas sobre esos sistemas. Esta supervisión y participación humana se someten a pruebas periódicas y funcionan de manera efectiva en los ejercicios internos del «equipo rojo».

Incentivos de diseño

Se alinean con los incentivos naturales de AWS y sus empleados. En algunos entornos, surge de forma natural una jerarquía de acceso, en la que unos pocos administradores tienen acceso completo a muchos sistemas de la empresa, entre los que suelen encontrarse los sistemas que controlan el acceso a otros sistemas. Sin embargo, los empleados de AWS no tienen ningún motivo para tener ese acceso a los datos de los clientes. Va en contra de sus objetivos empresariales que los empleados obtengan ese acceso. El diseño del sistema Nitro y su desarrollo y despliegue respaldan el incentivo de que no haya ninguna forma de que ningún empleado tenga acceso a los datos de los clientes. Los procesos internos del personal de AWS que definen la identidad de los empleados también reflejan y respaldan estos incentivos.

Documentación pública del sistema Nitro

Hay mucha información sobre el diseño del sistema Nitro disponible en diversos lugares.

- El diseño de seguridad de AWS Nitro System. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Código de arranque de verificación de modelos de los centros de datos de AWS. https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019: Security Benefits of the Nitro Architecture (Ventajas de la seguridad de la arquitectura Nitro) (SEP401-R). https://www.youtube.com/watch?v=kN9XcFp5vUM

3 Declaraciones

Declaraciones del diseño de seguridad de los productos

AWS manifiesta que los hosts del sistema Nitro de producción se adherirán a una política explícita de protección de la privacidad de los datos de los clientes con las siguientes declaraciones:

1. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube inicie sesión en el host subyacente.
2. Ninguna API administrativa puede acceder al contenido del cliente en el host subyacente.
3. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube acceda al contenido del cliente almacenado en el almacenamiento de instancias y en los volúmenes de EBS cifrados.
4. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube acceda a los datos cifrados transmitidos a través de la red.
5. El acceso a las API administrativas siempre requiere autenticación y autorización.
6. El acceso a las API administrativas siempre se registra.
7. Los hosts solo pueden ejecutar software probado y firmado que se despliegue mediante un servicio de despliegue autenticado y autorizado. Ningún empleado de un proveedor de servicios en la nube puede desplegar código directamente en los hosts.

Análisis de las declaraciones

1. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube inicie sesión en el host subyacente.

Por diseño, los sistemas no exponen ningún mecanismo que pueda proporcionar acceso a una línea de comando o cualquier otro mecanismo similar para la ejecución de comandos arbitrarios. No hay forma de habilitar o desplegar un mecanismo de este tipo. No existen mecanismos excepcionales o externos que proporcionen esta capacidad.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. No hay indicios de que un empleado de un proveedor de servicios en la nube pueda obtener dicho acceso o un acceso equivalente a ningún host.

2. Ninguna API administrativa puede acceder al contenido del cliente en el host subyacente.

Las API administrativas no realizan ninguna actividad que permita acceder o revelar el contenido del cliente. No hay ninguna API que pueda provocar que el contenido se traslade a otra ubicación a la que se pueda acceder. No hay ninguna API que reduzca o elimine las protecciones del contenido del cliente.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. Las API administrativas no pueden acceder al contenido del cliente en el host subyacente. Esa funcionalidad no existe.

3. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube acceda al contenido del cliente almacenado en el almacenamiento de instancias y en los volúmenes de EBS cifrados.

La API administrativa no incluye ninguna funcionalidad que proporcione acceso al contenido del cliente en el almacenamiento de instancias. No es posible utilizar la API para crear condiciones en las que esto sea posible. Todos los elementos de almacenamiento de instancias están cifrados en reposo, al igual que los volúmenes de EBS cifrados.

Los volúmenes de almacenamiento de EBS sin cifrar siguen siendo una opción para los clientes.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. No existe ningún mecanismo mediante el cual un empleado de un proveedor de servicios en la nube pueda acceder al contenido del cliente almacenado en instancias de host o en volúmenes de EBS cifrados.

4. No existe ningún mecanismo para que un empleado de un proveedor de servicios en la nube acceda a los datos cifrados transmitidos a través de la red.

El cifrado que se utiliza para proteger los datos relacionados con Nitro y otros tipos de cifrado gestionados por AWS utiliza los algoritmos adecuados y una gestión de claves segura. Se utiliza el protocolo TLS 1.2 para establecer conexiones cifradas. Las claves utilizadas directamente por el hardware Nitro se almacenan en un almacenamiento cifrado local protegido por un chip TPM a prueba de manipulaciones. Todas las comunicaciones de API administrativas y las comunicaciones administradas por AWS se cifran de forma segura. AWS utiliza variantes de algoritmos y versiones de protocolos seguros y puede migrar rápidamente a versiones más recientes según sea necesario.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. No existe ningún mecanismo para que los empleados de los proveedores de servicios en la nube accedan a las claves de cifrado o deshabiliten el cifrado de las comunicaciones.

5. El acceso a las API administrativas siempre requiere autenticación y autorización.

Las API administrativas requieren que las solicitudes contengan un token portador que proporcione datos de autenticación y autorización. Estos tokens se generan y se proporcionan a un operador autorizado de acuerdo con la identidad de ese operador y los derechos de acceso que tiene asociados. Los tokens solo otorgan acceso a los recursos para los que se emiten y caducan al poco tiempo. Los derechos de acceso se describen mediante la asociación de grupos de operadores con API específicas y conjuntos de recursos gestionados. Los derechos de acceso están limitados por las cuotas de los recursos afectados en un período determinado.

Los derechos de la configuración de los datos se auditan rápidamente y no son excesivamente complejos, para conseguir que los usuarios no tengan derechos excesivos ni inapropiados. Los datos de configuración de derechos de acceso se definen con el servicio del proveedor de tokens y siguen los mismos procedimientos de revisión por pares y control de cambios.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. El sistema de token portador implementado evita que un usuario malintencionado reutilice el token de forma distinta a su intención autorizada. Los plazos de caducidad de los tokens son lo bastante largos para evitar problemas si se interrumpe el servicio de emisión, pero lo bastante cortos como para limitar el uso indebido. Al localizar la configuración de los derechos de acceso con el código para el sistema que proporciona los tokens portadores se garantiza que ambos tengan la misma protección de procedimiento frente a alteraciones malintencionadas. Las cuotas impiden que un mal uso del acceso autorizado afecte a un número excesivo de sistemas.

6. El acceso a las API administrativas siempre se registra.

Todos los eventos de acceso, incluidos los errores de autenticación o autorización de solicitudes, se registran inmediatamente en una secuencia de registro de CloudWatch dedicada, creada y gestionada por el equipo de desarrollo de AWS Nitro. Estos eventos se supervisan en todo momento para detectar cualquier actividad o patrón de actividad claramente inusual o sospechoso.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. El proceso de supervisión está configurado para identificar las solicitudes que podrían indicar un abuso por parte de un agente malintencionado o un uso inapropiado de las API administrativas.

7. Los hosts solo pueden ejecutar software probado y firmado que se despliegue mediante un servicio de despliegue autenticado y autorizado. Ningún empleado de un proveedor de servicios en la nube puede desplegar código directamente en los hosts.

La protección de la integridad del software y los mecanismos de actualización automática del entorno Nitro están presentes desde el momento de la fabricación. El proceso mediante el cual los sistemas arrancan, adquieren identidad y realizan funciones de carga y administración de software de nivel superior está protegido desde este momento original. Es posible devolver de forma funcional un componente Nitro a su estado seguro inicial. Una vez recuperado dicho estado, se le puede asignar una identidad tanto en entornos de producción como de otro tipo. No es posible mover un componente a otro entorno, debido a los controles tanto de los componentes de Nitro como de los entornos.

Análisis: NCC Group considera que la arquitectura del sistema Nitro respalda plenamente esta declaración. Los procedimientos y las prácticas utilizados para desarrollar y autorizar el software no permitían que ningún agente malintencionado, ni siquiera con acceso de un operador de AWS o un desarrollador de Nitro, introdujera funciones no autorizadas en el sistema. Los incentivos de todas las personas autorizadas se alinean para evitar que esto ocurra.

4 Documentos revisados

Durante esta evaluación, se revisaron los siguientes documentos.

Documentación pública de AWS

Estos documentos están a disposición del público en general y se recomienda consultarlos para obtener una comprensión más completa del sistema Nitro.

- El diseño de seguridad de AWS Nitro System. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Código de arranque de verificación de modelos de los centros de datos de AWS. https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019: Security Benefits of the Nitro Architecture (Ventajas de la seguridad de la arquitectura Nitro) (SEP401-R). https://www.youtube.com/watch?v=kN9XcFp5vUM

Documentación interna de AWS

Estos documentos internos de AWS se guardaron en un sistema de AWS para su lectura y no se hicieron copias.

- **Documento de controles de Nitro**: documentación exhaustiva sobre el diseño del sistema Nitro en la que se recogen los controles para evitar que el operador acceda al contenido del cliente. El contenido de este documento incluía una descripción general detallada del sistema Nitro y sus componentes, una descripción de la base de computación de confianza (TCB), una descripción del funcionamiento de las API de Nitro, modelos de amenazas y mucho más.
- **Diseño de seguridad de Nitro**: documento de diseño inicial que recogía los objetivos de diseño y las limitaciones del sistema Nitro.
- **Infraestructura de clave pública de EC2**: documentación sobre la infraestructura de clave pública que proporciona la base de confianza entre los componentes internos de EC2.
- **Contenido de los tokens portadores**: documentación específica en la que se recoge la estructura de los tokens portadores que se utilizan en el sistema Nitro.
- **Canalización de Nitro**: documentación sobre el agente de orquestación utilizado para los despliegues de software de Nitro. La canalización de Nitro es el puente entre las herramientas estándar de Amazon, el servicio de conjuntos de pruebas y otros servicios y herramientas de EC2. Se han modificado algunas partes de este documento.