Affirmations sur les API et la sécurité d'AWS Nitro System

Amazon Web Services, Inc.
Version 1.0 – 11 avril 2023

Préparé par
John Redford
Xiang Wen Kuan

Préparé pour
Amazon Web Services

1 Synthèse

Synopsis

Au cours du dernier trimestre 2022, Amazon Web Services (AWS) a demandé à NCC Group d'effectuer une revue de l'architecture et de la conception d'AWS Nitro System, en se concentrant sur les affirmations spécifiques d'AWS concernant la sécurité des API de Nitro System. La planification et l'exécution de ces travaux se sont poursuivies au cours du premier trimestre 2023.

Voici une description de Nitro System, tirée de la documentation publique[1] :

> AWS Nitro System est une combinaison de conceptions de serveurs dédiés, de processeurs de données, de composants de gestion du système et de micrologiciels spécialisés qui fournissent la plateforme sous-jacente de toutes les instances Amazon EC2 lancées depuis le début 2018. Les trois composants clés du système Nitro sont les suivants :
>
> - Cartes Nitro dédiées : composants matériels conçus par AWS qui assurent le contrôle global du système et la virtualisation des entrées/sorties (E/S) indépendamment de la carte mère, de ses processeurs et de sa mémoire.
> - Puce de sécurité Nitro : permet un processus de démarrage sécurisé pour l'ensemble du système, basé sur un matériel racine de confiance, la capacité à proposer des instances bare metal, ainsi qu'une défense en profondeur qui protège le serveur contre toute modification non autorisée du micrologiciel du système.
> - Hyperviseur Nitro : hyperviseur délibérément minimal, semblable à un micrologiciel, conçu pour isoler fortement les ressources et offrir des performances quasiment impossibles à distinguer de celles d'un serveur bare metal.

AWS vérifie plusieurs affirmations de sécurité concernant la manière dont Nitro System est conçu pour empêcher les employés d'AWS d'accéder aux données des clients. Ces affirmations sont énumérées dans la section Affirmations du présent rapport.

Le Nitro System a été conçu pour atteindre les objectifs de sécurité répondant à ces exigences en fournissant une infrastructure complète d'administration, de gestion et de surveillance du système qui fonctionne depuis le niveau matériel jusqu'au provisionnement, au déploiement et à la fin de vie des systèmes. AWS ne dispose d'aucun chemin d'accès secondaire ou alternatif aux systèmes hôtes Nitro EC2. Ce niveau de rigueur et l'alignement approprié des objectifs de sécurité avec des pratiques commerciales durables et réalisables ont permis à AWS de concevoir un système capable de répondre aux demandes de sécurité et de confidentialité très strictes des clients.

En ce qui concerne la conception, NCC Group n'a trouvé aucune lacune dans le système Nitro susceptible de remettre en cause ces affirmations de sécurité. Toutes les conceptions impliquent des compromis, et AWS a choisi une conception dans laquelle l'impact d'une compromission malveillante serait similaire à celui d'une panne matérielle à petite échelle.

Logistique du projet

L'analyse a porté sur la vérification d'un certain nombre d'affirmations de sécurité concernant la conception des API d'administration de Nitro, ainsi que sur les processus de développement et d'administration qui créent et gèrent les API Nitro. Les opérateurs AWS utilisent les API Nitro pour effectuer un ensemble de tâches bien définies. Cela a porté sur le développement et le déploiement des éléments logiciels de Nitro System, l'infrastructure qu'il utilise et les procédures de création et de déploiement d'un

1. Conception de la sécurité d'AWS Nitro System https://docs.aws.amazon.com/whitepapers/latest/ security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html.

environnement AWS Nitro System.

Le cadre de l'évaluation mené par NCC Group comprenait :

- L'API de Nitro System, ses requêtes, ses fonctionnalités, ses processus de développement et de déploiement, ainsi que les éléments d'infrastructure connexes dont elle a besoin.
- Le rôle des opérateurs AWS qui disposent d'un accès autorisé aux API de Nitro System.
- Les employés non-opérateurs d'AWS, y compris les développeurs de Nitro System et le personnel qui gère et attribue des rôles aux employés.
- L'examen adéquat de Nitro System et de son environnement pour s'assurer qu'aucun autre système n'était présent ou n'était nécessaire en raison de sa conception.

Les éléments suivants n'entraient pas dans le cadre de l'évaluation :

- Évaluation générale des services de contrôle EC2.
- Évaluation de l'hyperviseur Nitro, du micrologiciel Nitro et du logiciel Nitro sur les Cartes Nitro.
- Évaluation des cartes Nitro.
- Évaluation de l'environnement physique et des contrôles de sécurité physique.

Méthodologie de l'évaluation

L'évaluation a été largement réalisée par le biais d'entretiens avec l'équipe de développement d'AWS Nitro et au travers de la documentation fournie par AWS. NCC Group a mené des entretiens avec plusieurs ingénieurs experimentés de l'équipe Nitro, dont l'ingénieur principal. Ces entretiens ont porté sur l'origine et les objectifs de conception du système, ainsi que sur ses caractéristiques opérationnelles et ses contraintes. En outre, des informations ont été fournies dans des documents et par partage d'écran afin de permettre à NCC Group de bien comprendre la sécurité de Nitro System. La documentation fournie couvrait de nombreux détails internes relatifs à la conception.

L'évaluation ne comprend pas l'examen approfondi de la mise en œuvre de composants spécifiques ni de tests pratiques ou de validation technique. L'évaluation des affirmations était basée sur l'analyse de la conception de Nitro System, telle qu'elle a été évaluée et observée, fournissant les moyens d'étayer ces affirmations et de garantir leur véracité. Dans la mesure où il s'agissait d'un examen au niveau de la conception, si cet objectif n'était pas atteint lors de la conception même, l'affirmation n'était pas considérée comme valide.

Limites du projet

Cet engagement représente une évaluation ponctuelle des API de Nitro System. Les menaces de sécurité et les techniques d'attaque évoluent rapidement et les résultats de cette évaluation ne constituent pas une approbation de l'adéquation des mesures de sécurité actuelles face aux menaces futures. En outre, les déclarations faites par NCC Group se réfèrent au système tel qu'il a été présenté au cours de la période d'évaluation et ne fournissent aucune assurance quant à des modifications techniques ou à des écarts futurs de politique choisis ou contraints. Bien que le processus de démarrage sécurisé et l'interaction des Cartes Nitro aient joué un rôle dans l'analyse, la sécurité de ces systèmes en présence d'un attaquant physique a été reportée à cette autre étude ou exclue du cadre de l'évaluation.

Cet examen est basé sur l'attestation du personnel AWS et les documents de conception du produit tels que présentés à NCC Group. Bien qu'AWS ait fourni une assistance appropriée à cet égard, NCC Group ne peut attester de l'exactitude des informations ou des conclusions associées, ni de la conformité de la mise en œuvre avec la conception. Toute déclaration concernant le fonctionnement d'AWS Nitro System fait référence à sa conception.

2 Conception de Nitro System

Introduction

NCC Group a effectué un examen de la conception architecturale de Nitro System qui a inclus plusieurs semaines de discussions et d'analyses, ainsi qu'une planification et un examen supplémentaire sur plusieurs mois. L'objectif de l'examen était de déterminer si l'architecture de Nitro System répondait aux exigences de sécurité d'AWS. L'équipe de consultants a examiné le système du point de vue des opérateurs AWS, des personnes ayant un accès non public à l'environnement, ainsi que des développeurs de Nitro System et d'autres employés d'AWS.

L'analyse a également révélé que ces API constituent le seul moyen pour les opérateurs AWS d'interagir avec les instances hôtes et qu'il n'existe aucun autre moyen de se connecter, d'ouvrir une session ou d'obtenir un autre type d'accès privilégié. L'analyse a également révélé qu'aucun employé AWS autre que les opérateurs ne peut utiliser ces API.

Objectifs de conception de Nitro System

Moindre privilège

La conception de Nitro System respecte le principe du moindre privilège. La conception incluait les interdictions suivantes :

- Accès aux données des clients.
- Accès pour exécuter des commandes ou du code arbitraires.
- Personnalisation d'une instance à l'aide de correctifs ou de versions logicielles uniques.
- Migration des données ou du stockage vers une autre instance ou un autre environnement.
- Activité non enregistrée.
- Procédures d'urgence pour contourner ou supprimer les dispositifs de sécurité.

La conception de Nitro System a été adaptée aux exigences essentielles des environnements en matière de gestion des événements de perte de disponibilité à petite échelle, tels que des pannes matérielles classiques ou un accident. L'ampleur des abus potentiels commis par un utilisateur malveillant aurait un impact similaire à celui de ces événements.

Redondance et confiance zéro

Les composants de Nitro System sont conçus pour effectuer des contrôles de sécurité redondants et multicouches. La conception garantit que l'authentification et l'autorisation sont vérifiées de multiples fois et que plusieurs chemins sont nécessaires pour que les modifications logicielles soient développées et déployées. Les hôtes d'instance sont conçus pour vérifier indépendamment les contrôles d'accès appropriés avant d'effectuer les actions demandées.

Confidentialité et intégrité

De solides contrôles de chiffrement et de signature sont présents tout au long de la conception de l'environnement. La conception globale de Nitro System consiste à s'assurer que toutes les communications de ce système sont chiffrées de manière sécurisée et que tous ses composants déployés sont signés et validés. Afin de réduire le risque de compromission des clés qui protègent les communications et les mises à jour logicielles, la conception garantit que la confiance repose sur des systèmes sécurisés qui ne dépendent pas de niveaux de contrôle d'accès inférieurs pour la gestion de la sécurité.

Audit et surveillance

Toutes les demandes d'API Nitro System sont enregistrées dans un environnement CloudWatch sécurisé avec des contrôles d'accès à plusieurs niveaux. Les journaux sont surveillés en permanence pour détecter l'utilisation de demandes sensibles ou de modèles d'activité visant à attirer l'attention humaine sur ces systèmes. Ce suivi et cet engagement humain sont régulièrement testés et fonctionnent efficacement dans le cadre d'exercices internes effectués par l'équipe "red team".

Avantages de la conception

Cela correspond aux motivations naturelles d'AWS et de ses employés. Dans certains environnements, une hiérarchie d'accès apparaît naturellement, une poignée d'administrateurs disposant d'un accès complet à de nombreux systèmes de l'entreprise, y compris souvent aux systèmes contrôlant l'accès à d'autres systèmes. Cependant, les employés d'AWS n'ont aucune raison de disposer d'un tel accès aux données des clients. Le fait que les employés obtiennent un jour cet accès va à l'encontre des objectifs commerciaux d'AWS. La conception de Nitro System, son développement et son déploiement sont autant d'éléments qui incitent les employés à ne pas avoir accès aux données des clients. Les processus internes du personnel d'AWS qui définissent l'identité des employés reflètent et soutiennent également ces motivations.

Documentation publique sur Nitro System

De nombreux détails sur la conception de Nitro System sont disponibles à plusieurs endroits.

- Conception de la sécurité d'AWS Nitro System. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Code de vérification au démarrage du modèle provenant des centres de données AWS. https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019 : avantages de l'architecture Nitro en matière de sécurité (SEP401-R). https://www.youtube.com/watch?v=kN9XcFp5vUM

3 Affirmations

Affirmations relatives à la sécurité des produits

AWS atteste que les hôtes Nitro System en production respecteront une politique explicite de protection de la confidentialité des données des clients, avec les affirmations suivantes :

1. Il n'existe aucun mécanisme permettant à un employé du fournisseur de services cloud de se connecter à l'hôte sous-jacent.
2. Aucune API d'administration ne peut accéder au contenu client sur l'hôte sous-jacent.
3. Il n'existe aucun mécanisme permettant à un employé d'un fournisseur de services cloud d'accéder au contenu client stocké sur le stockage d'instances et les volumes EBS chiffrés.
4. Il n'existe aucun mécanisme permettant à un employé d'un fournisseur de services cloud d'accéder aux données chiffrées transmises sur le réseau.
5. L'accès aux API d'administration nécessite toujours une authentification et une autorisation.
6. L'accès aux API d'administration est toujours enregistré.
7. Les hôtes peuvent uniquement exécuter des logiciels testés et signés déployés par un service de déploiement authentifié et autorisé. Aucun employé d'un fournisseur de services cloud ne peut déployer du code directement sur les hôtes.

Analyse des affirmations

1. Il n'existe aucun mécanisme permettant à un employé du fournisseur de services cloud de se connecter à l'hôte sous-jacent.

En raison de leur conception, les systèmes ne présentent aucun mécanisme permettant d'accéder à une interface logiciel ou à tout autre mécanisme similaire pour l'exécution de commandes arbitraires. Il n'existe aucun moyen d'activer ou de déployer un tel mécanisme. Il n'existe aucun mécanisme exceptionnel ou externe pour fournir cette capacité.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Rien n'indique qu'un employé d'un fournisseur de services cloud puisse obtenir un tel accès ou un accès équivalent à un hôte.

2. Aucune API d'administration ne peut accéder au contenu client sur l'hôte sous-jacent.

Les API d'administration n'effectuent aucune activité visant à accéder au contenu client ou à le révéler. Aucune API ne peut entraîner le déplacement du contenu vers un autre emplacement où il est possible d'y accéder. Il n'existe aucune API susceptible de réduire ou de supprimer les protections du contenu client.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Les API d'administration ne peuvent pas accéder au contenu client sur l'hôte sous-jacent. Cette fonctionnalité n'existe pas.

3. Il n'existe aucun mécanisme permettant à un employé d'un fournisseur de services cloud d'accéder au contenu client stocké sur le stockage d'instances et les volumes EBS chiffrés.

L'API d'administration n'inclut aucune fonctionnalité permettant d'accéder au contenu du client sur le stockage d'instances. Il n'est pas possible d'utiliser l'API pour créer les conditions dans lesquelles cela deviendrait possible. Les éléments de stockage d'instances sont tous chiffrés au repos, ainsi que les volumes EBS chiffrés.

Les volumes de stockage EBS non chiffrés existent toujours en tant que choix du client.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Il n'existe aucun mécanisme permettant à un employé d'un fournisseur de services cloud d'accéder au contenu client stocké sur des instances hôtes ou dans des volumes EBS chiffrés.

4. **Il n'existe aucun mécanisme permettant à un employé d'un fournisseur de services cloud d'accéder aux données chiffrées transmises sur le réseau.**

Le chiffrement utilisé pour protéger les données relatives à Nitro System et les autres méthodes de chiffrement gérées par AWS font appel à des algorithmes appropriés et à une gestion sécurisée des clés. Le protocole TLS 1.2 est utilisé pour négocier des connexions chiffrées. Les clés directement utilisées par le matériel de Nitro System sont stockées sur un support chiffré localement protégé par une puce TPM inviolable. Toutes les communications d'API d'administration et les communications gérées par AWS sont chiffrées de manière sécurisée. AWS utilise une version de protocole sécurisée et des variantes d'algorithmes et peut rapidement migrer vers des versions plus récentes si nécessaire.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Il n'existe aucun mécanisme permettant aux employés des fournisseurs de services cloud d'accéder aux clés de chiffrement ou de désactiver le chiffrement des communications.

5. **L'accès aux API d'administration nécessite toujours une authentification et une autorisation.**

Les API d'administration exigent que les demandes contiennent un jeton de porteur fournissant à la fois des données d'authentification et d'autorisation. Ces jetons sont générés et fournis à un opérateur autorisé conformément à l'identité de cet opérateur et aux droits d'accès qui lui sont associés. Les jetons ne donnent accès qu'aux ressources pour lesquelles ils sont émis et expirent rapidement. Les droits d'accès sont décrits par l'association de groupes d'opérateurs à des API spécifiques et à des ensembles de ressources gérées. Les droits d'accès sont limités par des quotas sur les ressources affectées au cours d'une période donnée.

Les données de configuration des droits elles-mêmes sont rapidement contrôlables et ne sont pas excessivement complexes, de sorte que les utilisateurs ne disposent pas de droits excessifs ou inappropriés. Les données de configuration des droits d'accès sont définies avec le service du fournisseur de jetons et suivent les mêmes procédures d'évaluation et de contrôle des modifications par des pairs.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Le système de jeton de porteur mis en œuvre empêche un utilisateur malveillant de réutiliser le jeton en dehors de son intention autorisée. Les délais d'expiration des jetons sont suffisamment longs pour éviter tout problème en cas d'interruption du service émetteur, mais suffisamment courts pour limiter les utilisations abusives. La localisation de la configuration des droits d'accès à l'aide du code du système qui fournit les jetons de porteur garantit que les deux bénéficient d'une protection procédurale égale contre les modifications malveillantes. Les quotas empêchent tout abus d'accès autorisé d'affecter un nombre déraisonnable de systèmes.

6. **L'accès aux API d'administration est toujours enregistré.**

Tous les événements d'accès, y compris l'échec de l'authentification ou de l'autorisation des demandes, seront immédiatement enregistrés dans un flux de journaux CloudWatch dédié créé et géré par l'équipe de développement AWS Nitro. Ces événements sont surveillés en permanence pour détecter toute activité ou tout schéma d'activité particulièrement inhabituel ou suspect.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Le processus de surveillance est configuré pour identifier les demandes qui indiqueraient un abus de la part d'un agent malveillant ou une utilisation inappropriée des API d'administration.

7. Les hôtes peuvent uniquement exécuter des logiciels testés et signés déployés par un service de déploiement authentifié et autorisé. Aucun employé d'un fournisseur de services cloud ne peut déployer du code directement sur les hôtes.

La protection de l'intégrité du logiciel et des mécanismes de mise à jour automatique de l'environnement de Nitro System sont présents dès la fabrication. Le processus par lequel les systèmes démarrent, acquièrent une identité et exécutent des fonctions de chargement et de gestion des logiciels de niveau supérieur est sécurisé à partir de ce point initial. Il est possible de rétablir fonctionnellement l'état sécurisé initial d'un composant de Nitro System. À partir de cette condition, il peut être identifié dans des environnements de production ou autres. Aucun déplacement d'un composant vers un autre environnement n'est possible, en raison des contrôles effectués à la fois dans les composants de Nitro System et dans les environnements.

Analyse : NCC Group estime que l'architecture de Nitro System valide pleinement cette affirmation. Les procédures et pratiques utilisées pour développer et autoriser les logiciels ne permettraient à aucun agent malveillant, même avec un accès opérateur AWS ou développeur Nitro, d'injecter des fonctionnalités non autorisées dans le système. Les incitations de toutes les personnes autorisées visent à empêcher que cela ne se produise.

4 Documents examinés

Les documents suivants ont été examinés au cours de cette évaluation.

Documentation publique AWS

Ces documents sont mis à la disposition du grand public et sont recommandés pour mieux comprendre le Nitro System.

- Conception de la sécurité d'AWS Nitro System. https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Code de démarrage de vérification du modèle provenant des centres de données AWS. https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019 : avantages de l'architecture Nitro en matière de sécurité (SEP401-R). https://www.youtube.com/watch?v=kN9XcFp5vUM

Documentation interne AWS

Ces documents internes d'AWS ont été conservés sur un système AWS à des fins de lecture et aucune copie n'a été faite.

- **Document de contrôles Nitro** : documentation de conception complète pour Nitro System couvrant les commandes destinées à empêcher l'opérateur d'accéder au contenu client. Le contenu de ce document comprenait une présentation détaillée de Nitro System et de ses composants, une description de la base informatique sécurisée (TCB), une description du fonctionnement des API Nitro, des modèles de menace, etc.
- **Conception de la sécurité Nitro** : premier document de conception qui traitait des objectifs et des contraintes de Nitro System.
- **Infrastructure à clé publique EC2** : documentation sur l'infrastructure à clé publique qui constitue la base de la confiance entre les composants internes d'EC2.
- **Contenu des jetons au porteur** : documentation spécifique concernant la structure des jetons du porteur utilisés par Nitro System.
- **Pipeline Nitro** : documentation sur l'agent d'orchestration utilisé pour les déploiements de logiciels Nitro. Le composant Pipeline Nitro fait le lien entre les outils Amazon standard, le service de suite de tests et les autres services et outils EC2. Certaines parties de ce document ont été expurgées.