Guide de l'administrateur

Amazon Nimble Studio

Amazon Nimble Studio: Guide de l'administrateur

Table of Contents

Avis de fin de support : le 22 octobre 2024, le support d'Amazon Nimble Studio AWS cessera. Après le 22 octobre 2024, vous ne pourrez plus accéder à la console Nimble Studio ni aux ressources de Nimble Studio.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.

Qu'est-ce qu'Amazon Nimble Studio ?

Nimble Studio fournit une infrastructure et une gestion centralisée pour une suite d'applications et de services que les artistes peuvent utiliser pour produire des effets visuels, des animations et du contenu de jeux dans le cloud.

Avec Nimble Studio, vous disposez d'outils essentiels pour la gestion des utilisateurs et des groupes. Vous pouvez également ajouter et gérer des applications, notamment AWS Thinkbox et Nimble Studio File Transfer.

Nimble Studio dispose d'une interface unifiée qui réunit toutes les ressources de votre studio au même endroit. Vous pouvez intégrer des utilisateurs, attribuer des applications et associer des autorisations spécifiques à leur fonction. Nimble Studio ne nécessite aucune AWS expérience et vous pouvez le configurer en cinq minutes environ.

Table des matières

Fonctionnalités et avantages

Voici quelques-unes des fonctionnalités et des avantages que vous offre Nimble Studio :

- Utilisez Nimble Studio gratuitement ; ne payez que pour les ressources de studio utilisées par vos applications.
- Gérez votre studio de manière centralisée, vérifiez son statut et obtenez des informations de haut niveau sur son fonctionnement.
- Ajoutez et gérez les applications, les utilisateurs et les groupes Nimble Studio, et associez des autorisations.
- Gérez en toute sécurité l'accès aux ressources du studio à l'aide de politiques et de rôles AWS Identity and Access Management (IAM).
- Gérez la sécurité de connexion pour les utilisateurs du studio et les fournisseurs d'identité externes avec AWS IAM Identity Center (IAM Identity Center).

- Organisez et retrouvez facilement les ressources de votre studio à l'aide de balises renvoyant aux ressources de votre studio.

Applications associées

Nimble Studio fournit des applications permettant aux créateurs de contenu numérique d'exploiter un studio basé sur le cloud pour produire des effets visuels (VFX), des animations et du contenu interactif.

Vous pouvez installer ces applications sur votre ordinateur local ou dans le cloud avec une instance Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez également utiliser Amazon Simple Storage Service (Amazon S3) pour transférer et stocker des ressources multimédia numériques en toute sécurité. Cela signifie que vous pouvez utiliser Nimble Studio pour réduire les coûts liés à l'infrastructure physique, à l'équipement et au personnel technique.

Nimble Studio propose actuellement les applications suivantes :

- AWS Thinkbox: Thinkbox le logiciel inclut le gestionnaire de ferme de rendu Thinkbox Deadline, et le plugin 3D, Thinkbox Krakatoa. Vous pouvez utiliser … Thinkbox un logiciel pour vous aider à augmenter la production créative de votre studio sur site, dans le cloud avec Amazon EC2, ou une combinaison des deux. Pour plus d'informations, consultez .AWS Thinkbox Des produits.
- Nimble Studio File Transfer: File Transfer accélère les transferts de ressources multimédias numériques vers et depuis Amazon S3. File Transfer fournit une interface utilisateur graphique que vous pouvez utiliser pour déplacer rapidement des milliers de fichiers multimédias volumineux. Pour plus d'informations, consultez la section Qu'est-ce que Nimble Studio File Transferpage.

Tarification de Nimble Studio

La configuration de Nimble Studio et son utilisation pour gérer l'infrastructure, les utilisateurs, la sécurité et les services de votre studio sont gratuits.

Toutefois, si vous configurez des services et des applications dans votre studio, des frais de stockage et d'autres ressources du studio peuvent vous être facturés. Pour plus d'informations sur la tarification des applications Nimble Studio, consultez la page de tarification de chaque application.

Pour plus d'informations sur la gestion de vos AWS coûts, consultez le AWS Cost Explorer Serviceet AWS Budgets.

Commencez avec Nimble Studio

La configuration et le déploiement de Nimble Studio prennent environ cinq minutes.

Après vous être familiarisé avec les concepts et la terminologie de Nimble Studio, consultez Getting started with Amazon Nimble Studio. Vous y trouverez des step-by-step instructions pour déployer votre studio.

Concepts et terminologie pour Amazon Nimble Studio

Pour vous aider à démarrer avec Amazon Nimble Studio et à comprendre son fonctionnement, vous pouvez consulter les principaux concepts et termes de ce guide.

Fonctions principales

Amazon Nimble Studio

Amazon Nimble Studio permet aux studios de création de produire des effets visuels, des animations et du contenu interactif entièrement dans le cloud, de l'esquisse du storyboard au livrable final.
Service AWS

Console Amazon Nimble Studio

La console Nimble Studio est une partie de la AWS Management Consoleconsole dédiée à nos clients informatiques administratifs. C'est sur cette console que les administrateurs créent leur studio cloud et gèrent de nombreux paramètres. Par exemple, la page Studio Manager vous permet d'ajouter ou de supprimer des ressources, d'ajouter des applications et d'accorder des autorisations aux utilisateurs et aux groupes.

Portail Amazon Nimble Studio

Le portail Nimble Studio fournit une interface utilisateur pour day-to-day les interactions avec les applications et les services Nimble Studio. Les utilisateurs se connectent directement au portail avec leur nom d'utilisateur et leur mot de passe sans avoir à interagir avec le AWS Management Console.

Nimble Studio File Transfer

File Transfer accélère les transferts de ressources multimédias numériques vers et depuis Amazon Simple Storage Service (Amazon S3). File Transfer fournit une interface utilisateur graphique que vous pouvez utiliser pour déplacer rapidement des milliers de fichiers multimédias volumineux. Pour plus d'informations, consultez la section Qu'est-ce que Nimble Studio File Transferpage.

AWS Thinkbox

Thinkbox le logiciel inclut le gestionnaire de ferme de rendu Thinkbox Deadline, et le plugin 3D, Thinkbox Krakatoa. Vous pouvez utiliser … Thinkbox un logiciel pour vous aider à augmenter la production créative de votre studio sur site, dans le cloud avec Amazon EC2, ou une combinaison des deux. Pour plus d'informations, consultez .AWS Thinkbox Produits.

Concepts clés et terminologie

AWS politiques gérées

Une politique AWS gérée est une politique autonome créée et administrée par AWS. Ces politiques sont dites autonomes, ce qui signifie que chaque politique a son propre Amazon Resource Name (ARN) incluant le nom de la politique. Par exemple, arn:aws:iam : IAMRead OnlyAccess :aws:policy/ est une politique gérée. AWS Pour plus d'informations sur ARNs, consultez IAM ARNs.

AWS les politiques gérées sont utilisées pour accorder des autorisations aux fonctions de travail courantes. Les politiques relatives aux fonctions de travail sont maintenues et mises à jour AWS lorsque de nouveaux services et opérations d'API sont introduits. Par exemple, la fonction AdministratorAccessjob fournit un accès complet et une délégation d'autorisations à chaque service et ressource qu'il contient AWS. Alors que les politiques de AWS gestion de l'accès partiel telles qu' AmazonMobileAnalyticsWriteOnlyAccessAmazon EC2 ReadOnlyAccess peuvent fournir des niveaux d'accès spécifiques Services AWS sans autoriser l'accès complet. Pour en savoir plus sur les politiques d'accès, voir Comprendre les résumés des niveaux d'accès dans les résumés des politiques.

AWS Management Console

AWS Management ConsoleIl s'agit d'une application Web qui donne accès à une vaste collection de consoles de service pour la gestion Services AWS.

Chaque service inclut également sa propre console. Ces consoles proposent une large gamme d'outils pour le cloud computing. Il existe même un service qui facilite la facturation et la gestion des coûts.

AWS IAM Identity Center (Centre d'identité IAM)

IAM Identity Center est un AWS service qui facilite la gestion centralisée de l'accès à de multiples Comptes AWS applications professionnelles. Avec IAM Identity Center, vous pouvez fournir aux utilisateurs un accès par authentification unique à tous les comptes et applications qui leur sont attribués à partir d'un seul endroit. Vous pouvez également gérer de manière centralisée l'accès à plusieurs comptes et les autorisations des utilisateurs pour tous vos comptes. AWS Organizations Pour plus d'informations, consultez AWS IAM Identity Center FAQs.

AWS PrivateLink

AWS PrivateLink fournit une connectivité privée entre VPCs Services AWS, et vos réseaux locaux, sans exposer votre trafic à l'Internet public. AWS PrivateLink permet de connecter facilement les

services entre différents comptes et VPCs. AWS PrivateLinkest disponible moyennant des frais mensuels qui vous Compte AWS sont facturés.

Création de contenu numérique (DCC)

La création de contenu numérique (DCC) fait référence à la catégorie d'applications utilisées pour produire du contenu créatif, notamment Blender, Nuke, Maya, et Houdini.

Régions

Nimble Studio propose onze options Régions AWS parmi lesquelles choisir pour déployer votre studio. Les régions sont celles où se trouvent les infrastructures de studio essentielles, telles que vos données et vos applications.

La région doit être située le plus près des utilisateurs de votre studio. Cela réduit le décalage et améliore les vitesses de transfert de données.

Studio

Un studio est le conteneur de premier niveau pour les autres ressources liées à Nimble Studio. Votre studio cloud gère le portail Web Nimble Studio et les connexions aux ressources essentielles de votre entreprise, Compte AWS telles que votre VPC, votre répertoire d'utilisateurs et les clés de chiffrement du stockage.

Applications de studio

Les composants Studio sont des configurations au sein de Nimble Studio d'un client qui indiquent au service comment accéder aux ressources telles que les systèmes de fichiers, les serveurs de licences et les fermes de rendu de votre Compte AWS entreprise.

Nimble Studio contient un certain nombre de sous-types de composants de studio, notamment un système de fichiers partagé, une ferme de calcul, Active Directory et un composant de licence. Ces sous-types décrivent les ressources que vous souhaitez que votre studio utilise.

Ressources du studio

Les ressources de studio sont un terme qui résume les besoins d'un studio dans ses activités quotidiennes. Lorsque l'on décrit la manière dont les ressources s'intègrent à l'infrastructure d'un studio cloud, elles peuvent également être appelées composants de studio.

Balises

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est composée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos AWS ressources de différentes manières. Par exemple, vous pouvez définir un ensemble de balises pour les instances Amazon Elastic Compute Cloud (Amazon EC2) de votre compte afin de suivre le propriétaire et le niveau de stack de chaque instance. Les balises vous permettent également d'intégrer les systèmes de fichiers partagés et les fermes de rendu de votre entreprise à Nimble Studio, afin de garantir la continuité de vos flux de travail pendant que vous déplacez votre personnel vers le cloud.

Les balises vous permettent de classer vos AWS ressources par objectif, propriétaire ou environnement. Cela est utile lorsque vous disposez de nombreuses ressources du même type : vous pouvez rapidement identifier une ressource spécifique en fonction des balises que vous lui avez attribuées.

Configuration de Nimble Studio

Ce didacticiel est destiné aux utilisateurs administrateurs qui souhaitent configurer un Amazon Nimble Studio.

Les sections suivantes vous guideront à travers les étapes à suivre avant de déployer un studio dans Nimble Studio.

Table des matières

Configurer IAM

Consultez la documentation AWS Identity and Access Management (IAM) suivante avant de commencer.

- Bonnes pratiques de sécurité dans IAM
- Connectez-vous à votre compte en Compte AWS tant qu'administrateur pour terminer le reste de la configuration.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un

utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et le gérer en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu’utilisateur doté d’un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l’URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l’utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d’un accès à d’autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d’autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center .

Ressources connexes

- Bonnes pratiques de sécurité en matière d'IAM
- Service AWS quotas - Références générales AWS

Commencer à utiliser Amazon Nimble Studio

Ce chapitre explique comment utiliser la console Nimble Studio pour créer l'infrastructure de votre studio, confirmer Région AWS, vérifier les paramètres et créer votre studio. Vous pouvez également personnaliser votre configuration à l'aide de paramètres supplémentaires.

Pour les nouveaux AWS clients, consultez les Configuration de Nimble Studio didacticiels.

Rubriques

Configuration de Nimble Studio

Ce guide vous explique comment configurer votre infrastructure, revoir vos paramètres et créer votre studio. Vous pouvez également personnaliser votre studio avecParamètres de studio supplémentaires.

Étape 1 : Configuration de l'infrastructure du studio

L'infrastructure de votre studio comprend les composants suivants :

- Nom d'affichage du studio : le nom d'affichage du studio vous permet d'identifier votre studio, par exemple AnyCompany Studio. Le nom de votre studio détermine également l'URL de votre portail Studio. Vous pouvez modifier le nom d'affichage de Studio une fois la configuration terminée, à tout moment.
- URL du portail du studio : vous pouvez accéder à votre studio à l'aide de l'URL du portail du studio. L'URL est basée sur le nom d'affichage du Studio, par exemple https://anycompanystudio.awsapps.com. Vous pouvez modifier l'URL du portail Studio une fois la configuration terminée, à tout moment.
- Région AWS: Région AWSIl s'agit de l'emplacement physique d'un ensemble de centres de AWS données. Lorsque vous configurez votre studio, la région choisit par défaut l'emplacement le plus proche de chez vous. Vous devez modifier la région afin qu'elle soit la plus proche de vos utilisateurs. Cela réduit le décalage et améliore les vitesses de transfert de données.

> **Important**
>
> Vous ne pouvez pas changer de région une fois que vous avez terminé de configurer Nimble Studio.

Effectuez les tâches décrites dans cette section pour configurer l'infrastructure de votre studio.

Pour configurer l'infrastructure de votre studio

1. Connectez-vous à la console Nimble Studio AWS Management Consoleet ouvrez-la.
2. Choisissez Setup Nimble Studio, puis Next.
3. Entrez le nom d'affichage du studio, par exemple**`AnyCompany Studio`**.
4. (Facultatif) Pour modifier le nom du portail Studio, choisissez Modifier l'URL.
5. (Facultatif) Pour modifier la Région AWSzone la plus proche des utilisateurs de votre studio, choisissez Changer de région.
   a. Sélectionnez la région la plus proche de vos utilisateurs.
   b. Choisissez Appliquer la région.
6. (Facultatif) Pour personnaliser davantage la configuration de votre studio, sélectionnez Paramètres de studio supplémentaires.
7. Pour vérifier vos paramètres avant de créer votre studio, choisissez Next.

Étape 2 : Révisez et créez votre studio

Après avoir configuré l'infrastructure de votre studio, vous pouvez passer en revue, apporter des modifications et créer votre studio.

Pour revoir et créer votre studio

1. Sur la page Réviser et créer, passez en revue l'infrastructure de votre studio.
2. Vérifiez que c'Région AWSest le plus proche des utilisateurs de votre studio.
3. (Facultatif) Choisissez Modifier pour apporter des modifications à la configuration de votre studio.
4. Lorsque vous êtes prêt, choisissez Create studio.

Paramètres de studio supplémentaires

La configuration de Nimble Studio inclut des paramètres de studio supplémentaires. Grâce à ces paramètres, vous pouvez afficher toutes les modifications apportées par la configuration de Nimble Studio à votre compte Compte AWS, configurer votre rôle d'utilisateur de studio et modifier le type de clé de chiffrement. Vous pouvez également ajouter des balises facultatives aux ressources de votre studio.

Configurer le rôle d'utilisateur du studio

Un AWS service peut assumer un rôle de service pour effectuer des actions en votre nom. Nimble Studio nécessite un rôle d'utilisateur de studio pour permettre aux utilisateurs d'accéder aux ressources de votre studio.

Vous pouvez associer des politiques gérées AWS Identity and Access Management (IAM) au rôle d'utilisateur du studio. Les politiques permettent aux utilisateurs d'effectuer certaines actions, telles que la création de tâches dans une application Nimble Studio spécifique. Comme les applications dépendent de conditions spécifiques définies dans la stratégie gérée, si vous n'utilisez pas les politiques gérées, l'application risque de ne pas fonctionner comme prévu.

Vous pouvez modifier le rôle d'utilisateur du studio une fois la configuration terminée, à tout moment. Pour plus d'informations sur les rôles des utilisateurs, consultez la section Rôles IAM.

Les onglets suivants contiennent des instructions pour deux cas d'utilisation différents. Pour créer et utiliser un nouveau rôle de service, choisissez l'onglet Nouveau rôle de service. Pour utiliser un rôle de service existant, choisissez l'onglet Rôle de service existant.

New service role

Pour créer et utiliser un nouveau rôle de service

1. Sélectionnez Créer et utiliser un nouveau rôle de service.
2. (Facultatif) Entrez un nom de rôle d'utilisateur du service.
3. Choisissez Afficher les détails des autorisations pour plus d'informations sur le rôle.

Existing service role

Pour utiliser un rôle de service existant

1. Sélectionnez Utiliser un rôle de service existant.
2. Ouvrez la liste déroulante pour choisir un rôle de service existant.
3. (Facultatif) Choisissez Afficher dans la console IAM pour plus d'informations sur le rôle.

AWS IAM Identity Center

AWS IAM Identity Center est un service d'authentification unique basé sur le cloud pour la gestion des utilisateurs et des groupes. IAM Identity Center peut également être intégré à votre fournisseur d'authentification unique (SSO) d'entreprise afin que les utilisateurs puissent se connecter avec leur compte d'entreprise.

Nimble Studio active IAM Identity Center par défaut, et il est nécessaire pour configurer et utiliser Nimble Studio. Pour plus d'informations, reportez-vous à la section Qu'est-ce que c'est AWS IAM Identity Center.

Configuration de la clé AWS KMS de chiffrement

AWS Key Management Service Les clés (AWS KMS) sont le principal type de clé KMS que vous pouvez utiliser pour chiffrer, déchiffrer et rechiffrer vos données.

Nimble Studio inclut les types de clés AWS KMS de chiffrement suivants :

- AWS clé possédée : les clés AWS détenues sont des clés KMS que l'utilisateur Service AWS possède et gère pour une utilisation multiple Comptes AWS. AWS les clés détenues ne résident pas dans votre compte Compte AWS, mais Nimble Studio peut utiliser une clé AWS détenue pour protéger les ressources de votre compte.

  Pour l'utiliser AWS KMS, il n'est pas nécessaire de créer ou de maintenir la clé ou sa politique de clé. L'utilisation des clés que vous possédez est AWS gratuite et elles ne sont pas prises en compte dans les AWS KMS quotas de votre part Compte AWS.
- AWS KMS Clé gérée par le client — Une clé gérée par le client est une clé KMS Compte AWS que vous créez, détenez et gérez.

  Vous avez un contrôle total sur ces clés KMS. Les clés gérées par le client entraînent des frais mensuels. Ils sont également soumis à des frais pour chaque demande d'API AWS KMS au-delà du niveau gratuit. Pour plus d'informations sur la AWS KMS tarification, consultez la section AWS Key Management Service tarification.

Le type de clé de chiffrement ne peut pas être modifié une fois la configuration terminée. Pour plus d'informations sur les types de clés de chiffrement AWS KMS et les types de clés de chiffrement, consultez la AWS KMS documentation.

Pour choisir un autre type de clé de chiffrement

1. Sélectionnez Choisir une autre AWS KMS clé (avancé).
2. Sélectionnez une AWS KMS clé ou entrez un numéro de ressource Amazon (ARN).
3. Choisissez Créer une AWS KMS clé.

Configuration des balises

Les tags servent d'étiquettes pour organiser vos ressources Nimble Studio. Vous pouvez ajouter jusqu'à 50 balises pour identifier, organiser, filtrer et rechercher des ressources.

Chaque balise se compose de deux parties, que vous définissez : une clé de balise et une balise facultative Value, par exemple, clé : `domain` et valeur :`anycompanystudio.com`.

Vous pouvez à tout moment ajouter ou supprimer des balises une fois la configuration terminée. Pour plus d'informations sur les balises, consultez la section Marquage de vos AWS ressources.

Pour ajouter des balises aux ressources de votre studio

1. Sélectionnez Add new tag (Ajouter une nouvelle balise).
2. Saisissez la clé de balise.
3. (Facultatif) Entrez la valeur du tag.

Supprimer un studio

Si vous n'avez plus besoin d'un studio, vous pouvez le supprimer. Lorsque vous supprimez votre studio, seule l'infrastructure du studio est supprimée. Vos autres AWS ressources, telles que les rôles d'utilisateur, les politiques et les données d'application, restent intactes.

> **Important**
>
> Vous ne pouvez pas restaurer un studio après l'avoir supprimé.

Pour supprimer votre studio

1. Connectez-vous à la console Nimble Studio AWS Management Console et ouvrez-la.
2. Sélectionnez Vue d'ensemble du studio.
3. Choisissez Actions, puis sélectionnez Supprimer le studio.
4. Entrez**`delete`**, puis choisissez Supprimer.

Sécurité dans Amazon Nimble Studio

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Nimble Studio, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

> **Important**
>
> Il est vivement recommandé de lire et de vous familiariser avec le Security Pillar - AWS Well-Architected Framework. Cet article contient les principes clés pour sécuriser votre AWS infrastructure.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation Nimble Studio. Les rubriques suivantes expliquent comment configurer Nimble Studio pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser votre Nimble Studio ressources.

En savoir plus

- Pilier de sécurité - AWS Well-Architected Framework
- Sécurité pour le AWS Cloud Development Kit (AWS CDK) (AWS CDK)

- Sécurité dans Amazon Virtual Private Cloud
- AWS informations d'identification de sécurité
- Sécurité sur Amazon EC2
  - Linux
  - Windows

Configurer la Compte AWS sécurité

Ce guide explique comment configurer votre système Compte AWS pour recevoir des notifications lorsque vos ressources sont compromises et pour autoriser des Compte AWS utilisateurs spécifiques à y accéder. Pour sécuriser Compte AWS et suivre vos ressources, procédez comme suit.

Table des matières

Supprimer les clés d'accès de votre compte

Vous pouvez autoriser l'accès programmatique à vos AWS ressources à partir du AWS Command Line Interface (AWS CLI) ou avec AWS APIs. Toutefois, il est AWS recommandé de ne pas créer ni utiliser les clés d'accès associées à votre compte root pour l'accès par programmation.

Si vous avez toujours des clés d'accès, nous vous recommandons de les supprimer et de créer un utilisateur. Accordez ensuite à cet utilisateur uniquement les autorisations nécessaires pour l'appel APIs que vous prévoyez d'appeler. Vous pouvez utiliser cet utilisateur pour émettre des clés d'accès.

Pour plus d'informations, consultez la section Gestion des clés d'accès pour vous Compte AWS dans le Références générales AWS guide.

Activation de l'authentification multifactorielle (MFA)

L'authentification multifactorielle (MFA) est une fonctionnalité de sécurité qui fournit une couche d'authentification en plus de votre nom d'utilisateur et de votre mot de passe.

Le MFA fonctionne comme suit : après vous être connecté avec votre nom d'utilisateur et votre mot de passe, vous devez également fournir une information supplémentaire à laquelle vous seul avez un accès physique. Ces informations peuvent provenir d'un appareil MFA dédié ou d'une application sur un téléphone.

Vous devez sélectionner le type de périphérique MFA que vous souhaitez utiliser dans la liste des appareils MFA pris en charge. S'il s'agit d'un périphérique matériel, conservez le dispositif MFA dans un endroit sûr.

Si vous utilisez un appareil MFA virtuel (comme une application téléphonique), pensez à ce qui pourrait se passer en cas de perte ou d'endommagement de votre téléphone. L'une des approches consiste à conserver le dispositif MFA virtuel que vous utilisez dans un endroit sûr. Une autre option consiste à activer plusieurs appareils en même temps ou à utiliser une option MFA virtuelle pour récupérer les clés de l'appareil.

Pour en savoir plus sur l'authentification multifactorielle, voir Activation d'un dispositif d'authentification multifactorielle virtuelle (MFA).

Ressources connexes

- Commencer à utiliser l'authentification multifactorielle
- Sécurisation de l'accès à l' AWS utilisation de la MFA

Activer CloudTrail dans tous Régions AWS

Vous pouvez suivre toutes les activités de vos AWS ressources en utilisant AWS CloudTrail. Nous vous recommandons de l'activer CloudTrail dès maintenant. Cela peut aider Support votre architecte de AWS solutions à résoudre ultérieurement un problème de sécurité ou de configuration.

Pour activer la CloudTrail connexion à tous Régions AWS, voir AWS CloudTrail Mise à jour : activer dans toutes les régions et utiliser plusieurs pistes.

Pour en savoir plus CloudTrail, voir Activer CloudTrail : enregistrer l'activité de l'API dans votre Compte AWS. Pour savoir comment CloudTrail surveille Nimble Studio, voirEnregistrement des appels Nimble Studio à l'aide de AWS CloudTrail.

Configurer Amazon GuardDuty et les notifications

Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les éléments suivants :

- Sources de données
- Journaux de flux Amazon VPC
- AWS CloudTrail journaux des événements de gestion
- CloudTrail Journaux d'événements liés aux données S3
- Journaux DNS

Amazon GuardDuty identifie les activités inattendues, potentiellement non autorisées et malveillantes au sein de votre AWS environnement. Les activités malveillantes peuvent inclure des problèmes tels que l'augmentation des privilèges, l'utilisation d'informations d'identification exposées ou la communication avec des adresses IP ou des domaines malveillants. Pour identifier ces activités, GuardDuty utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, et l'apprentissage automatique. Par exemple, GuardDuty peut détecter les EC2 instances Amazon compromises diffusant des logiciels malveillants ou minant des bitcoins.

GuardDuty surveille également le comportement Compte AWS d'accès pour détecter tout signe de compromission. Cela inclut les déploiements d'infrastructure non autorisés, tels que les instances déployées dans un Région AWS environnement qui n'a jamais été utilisé. Cela inclut également des appels d'API inhabituels, tels qu'une modification de la politique de mot de passe pour réduire la force du mot de passe.

GuardDuty vous informe de l'état de votre AWS environnement en produisant des résultats de sécurité. Vous pouvez consulter ces résultats dans la GuardDuty console ou via les CloudWatch événements Amazon.

Configuration d'une rubrique et d'un point de terminaison Amazon SNS

Suivez les instructions de la rubrique Configuration d'un Amazon SNS et du didacticiel relatif aux terminaux.

Organiser un EventBridge événement pour les GuardDuty résultats

Créez une règle pour EventBridge envoyer des événements pour tous les résultats GuardDuty générés.

Pour créer un EventBridge événement pour les GuardDuty résultats

1. Connectez-vous à la EventBridge console Amazon : https://console.aws.amazon.com/events/

2. Dans le volet de navigation, choisissez Règles. Puis, choisissez Create rule (Créer une règle).
3. Entrez un nom et une description pour la nouvelle règle. Ensuite, sélectionnez Suivant.
4. Laissez AWS les événements ou les événements EventBridge partenaires sélectionnés comme Source de l'événement.
5. Dans Modèle d'événement, choisissez les AWS services pour la source de l'événement. Ensuite, GuardDutypour les AWS services, et GuardDuty Finding pour le type d'événement. Il s'agit du sujet que vous avez créé dansConfiguration d'une rubrique et d'un point de terminaison Amazon SNS.
6. Choisissez Suivant.
7. Pour Target 1, sélectionnez le AWS service. Choisissez le sujet SNS dans le menu déroulant Sélectionnez une cible. Choisissez ensuite le sujet de votre GuardDuty_to_email.
8. Dans la section Paramètres supplémentaires : utilisez le menu déroulant Configurer l'entrée cible pour choisir Transformateur d'entrée. Sélectionnez Configurer le transformateur d’entrée.
9. Entrez le code suivant dans le champ Chemin d'entrée de la section Transformateur d'entrée cible.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. Pour formater l'e-mail, entrez le code suivant dans le champ Modèle.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Sélectionnez Create (Créer). Ensuite, sélectionnez Suivant.
12. (Facultatif) Ajoutez des balises si vous utilisez des balises pour suivre vos AWS ressources.
13. Choisissez Suivant.

14. Passez en revue votre règle. Puis, choisissez Create rule (Créer une règle).

Maintenant que vous avez configuré votre système de Compte AWS sécurité, vous pouvez accorder l'accès à des utilisateurs spécifiques et recevoir des notifications lorsque vos ressources sont compromises.

Protection des données dans Amazon Nimble Studio

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Nimble Studio. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d’informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d’informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Nimble Studio ou autre Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d’informations d’identification dans l’adresse URL permettant de valider votre demande adressée à ce serveur.

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Nimble Studio. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. Il vous incombe de garder le contrôle sur votre contenu hébergé sur cette infrastructure. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour le Services AWS produit que vous utilisez.

Pour plus d’informations sur la confidentialité des données, consultez les FAQ sur la confidentialité des données. Pour plus d'informations sur la protection des données dans l'Union européenne, consultez le Centre du RGPD.

Chiffrement au repos

Nimble Studio protège les données sensibles du studio en les chiffrant au repos à l'aide des clés de chiffrement stockées dans AWS Key Management Service ()AWS KMS. Le chiffrement au repos est disponible partout Régions AWS où Nimble Studio est disponible. Les données de studio que nous chiffrons incluent le nom et les descriptions de tous les types de ressources, ainsi que les scripts des composants du studio, les paramètres des scripts, les points de montage, les noms de partage et d'autres données.

Le chiffrement des données signifie que les données sensibles enregistrées sur des disques ne sont pas lisibles par les utilisateurs ou les applications sans clé valide. Les données cryptées peuvent être stockées en toute sécurité au repos et ne peuvent être déchiffrées que par une partie ayant un accès autorisé à la clé gérée.

Pour plus d'informations sur la manière dont Nimble Studio utilise AWS KMS le chiffrement des données au repos, consultez. Gestion des clés pour Amazon Nimble Studio

Utiliser des subventions avec des AWS KMS clés

Une subvention est un instrument de politique qui permet aux AWS principaux d'utiliser des AWS KMS clés dans le cadre d'opérations cryptographiques. Il peut également leur permettre de consulter une clé KMS à l'aide de la commande`DescribeKey`, ainsi que de créer et de gérer des subventions.

Les subventions sont couramment utilisées par Services AWS ceux qui s'intègrent AWS KMS à pour chiffrer vos données au repos. Le service crée un octroi au nom d'un utilisateur du compte, utilise ses autorisations et retire l'octroi dès que sa tâche est terminée.

Lorsque Nimble Studio crée votre studio, nous attribuons deux rôles aux utilisateurs du portail Nimble Studio : les rôles d'utilisateur et d'administrateur. Nimble Studio octroie des autorisations sur des clés gérées par le client pour ces rôles afin de leur permettre d'accéder aux données chiffrées du studio.

> **Important**
>
> Si vous supprimez une subvention, le portail Nimble Studio sera inutilisable pour les utilisateurs, jusqu'à ce que l'administrateur crée une nouvelle subvention.

Pour plus de détails sur le Services AWS mode d'utilisation des autorisations, consultez la rubrique Comment Services AWS utiliser AWS KMS ou le chiffrement au repos dans le guide de l'utilisateur ou le guide du développeur du service.

Chiffrement en transit

Le tableau suivant fournit des informations sur le chiffrement des données en transit. Le cas échéant, d'autres méthodes de protection des données pour Nimble Studio sont également répertoriées.

Données	Chemin d'accès réseau	Protection
Ressources Web telles que des images et des JavaScript fichiers	Le chemin réseau relie les utilisateurs de Nimble Studio à Nimble Studio.	Le chiffrement des données utilise le protocole TLS 1.2 ou version ultérieure.
Pixels et trafic de streaming associé	Le chemin réseau relie les utilisateurs de Nimble Studio à Nimble Studio.	Chiffré à l'aide de la norme de chiffrement avancée 256 bits (AES-256) et transporté à

		l'aide du protocole TLS 1.2 ou version ultérieure.
Trafic API	Le chemin se situe entre les utilisateurs de Nimble Studio et Nimble Studio.	Chiffré à l'aide de TLS 1.2 ou version ultérieure. Les demandes de création de connexion sont signées à l'aide de SigV4.

Gestion des clés pour Amazon Nimble Studio

Lorsque vous créez un nouveau studio, vous pouvez choisir l'une des clés suivantes pour chiffrer les données de votre studio :

- AWS clé KMS détenue : type de chiffrement par défaut. La clé appartient à Nimble Studio (sans frais supplémentaires).
- Clé KMS gérée par le client : la clé est stockée dans votre compte et vous l'avez créée, détenue et gérée. Vous avez le contrôle total de la clé. AWS KMS des frais s'appliquent.

La suppression d'une clé KMS gérée par le client dans AWS Key Management Service (AWS KMS) est destructrice et potentiellement dangereuse. Il supprime de manière irréversible le contenu clé et toutes les métadonnées associées à la clé. Après la suppression d'une clé KMS gérée par le client, vous ne pouvez plus déchiffrer les données chiffrées par cette clé. Cela signifie que les données deviennent irrécupérables.

C'est pourquoi les AWS KMS clients disposent d'un délai d'attente pouvant aller jusqu'à 30 jours avant de supprimer la clé. La période d'attente par défaut est de 30 jours.

À propos de la période d'attente

Comme il est destructeur et potentiellement dangereux de supprimer une clé KMS gérée par le client, nous vous demandons de définir un délai d'attente de 7 à 30 jours. La période d'attente par défaut est de 30 jours.

Cependant, la période d'attente réelle peut être jusqu'à 24 heures plus longue celle que vous avez planifiée. Pour obtenir la date et l'heure réelles auxquelles la clé sera supprimée, utilisez l'DescribeKeyopération. Vous pouvez également voir la date de suppression planifiée d'une clé dans

la AWS KMS console sur la page détaillée de la clé, dans la section Configuration générale. Notez le fuseau horaire.

Pendant la période d'attente, le statut de la clé gérée par le client et l'état de la clé sont En attente de suppression.

- Une clé KMS gérée par le client en attente de suppression ne peut être utilisée dans aucune opération cryptographique.
- AWS KMS ne fait pas pivoter les clés de sauvegarde des AWS KMS clés gérées par le client en attente de suppression.

Pour plus d'informations sur la suppression d'une AWS KMS clé gérée par le client, voir Supprimer les clés principales du client.

Mesures de sécurité des données

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d’informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l’information fédérale).

Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles, telles que les numéros de compte client, dans des champs libres tels que le champ Nom. Cela inclut

lorsque vous travaillez avec Amazon Nimble Studio ou autre à Services AWS l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous saisissez dans Amazon Nimble Studio ou dans d'autres services peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Données diagnostiques et métriques

Lors du déploiement et de la suppression de StudioBuilder, Amazon Nimble Studio collecte certaines statistiques que nous utilisons pour diagnostiquer les problèmes et améliorer les fonctionnalités et l'expérience utilisateur de Nimble Studio.

Types de métriques collectées

- Informations d'utilisation – Commandes et sous-commandes génériques qui sont exécutées.
- Erreurs et informations de diagnostic : état et durée des commandes exécutées, y compris les codes de sortie, les noms des exceptions internes et les échecs.
- Informations sur le système et l'environnement — Version Python, système d'exploitation (Windows, Linux, ou macOS), ainsi que l'environnement dans lequel StudioBuilder il est exécuté.

Identity and Access Management pour Amazon Nimble Studio

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon Nimble Studio. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Nimble Studio.

Utilisateur du service : si vous utilisez le service Nimble Studio pour effectuer votre travail, vous êtes un utilisateur du service. Dans ce cas, votre administrateur vous fournira les informations d'identification et les autorisations dont vous avez besoin pour accéder aux ressources qui vous sont attribuées. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Nimble Studio pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Nimble Studio, consultezRésolution des problèmes d'identité et d'accès à Amazon Nimble Studio.

Administrateur du service — Si vous êtes responsable des ressources de Nimble Studio dans votre entreprise, vous avez probablement un accès complet à Nimble Studio. C'est à vous de déterminer les fonctionnalités et les ressources de Nimble Studio auxquelles vos employés doivent avoir accès. Soumettez ensuite des demandes à votre administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Nimble Studio, consultez. Comment Amazon Nimble Studio fonctionne avec IAM

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Pour plus d'informations sur la connexion à l'aide du AWS Management Console, consultez la section Connexion en AWS Management Console tant qu'utilisateur IAM ou utilisateur root dans le Guide de l'utilisateur IAM.

Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur Compte AWS root, en tant qu'utilisateur ou en assumant un rôle IAM. Vous pouvez également utiliser l'authentification unique de votre entreprise ou même vous connecter via Google ou Facebook. Dans ces cas, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide des informations d'identification d'une autre entreprise, vous assumez un rôle indirectement.

Pour vous connecter directement au AWS Management Console, utilisez votre mot de passe avec votre adresse e-mail d'utilisateur root ou votre nom d'utilisateur. Vous pouvez accéder AWS par programmation à l'aide de votre utilisateur root ou de vos clés d'accès utilisateur.

AWS fournit un SDK et des outils de ligne de commande pour signer cryptographiquement votre demande à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, signez vous-même la demande. Pour ce faire, utilisez Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour en savoir plus sur l'authentification des demandes, consultez Processus de signature Signature Version 4 dans Références générales AWS .

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Nous vous recommandons vivement de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes, même les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Utilisateurs et groupes

Un utilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Un utilisateur peut disposer d'informations d'identification à long terme ou d'un ensemble de clés d'accès. Pour savoir comment générer des clés d'accès, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Lorsque vous générez des clés d'accès pour un utilisateur, visualisez et enregistrez en toute sécurité la paire de clés. Vous ne pourrez pas récupérer la clé d'accès secrète à l'avenir. Générez plutôt une nouvelle paire de clés d'accès.

Un groupe IAM est une identité qui spécifie un ensemble d'utilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d’utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Quand créer un utilisateur (au lieu d'un rôle) dans le guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Il est similaire à un utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation des rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Autorisations utilisateur temporaires : un utilisateur peut endosser un rôle IAM pour accepter différentes autorisations temporaires concernant une tâche spécifique.
- Accès utilisateur fédéré : au lieu de créer un utilisateur, vous pouvez utiliser des identités existantes provenant du AWS Directory Service répertoire des utilisateurs de votre entreprise ou d'un fournisseur d'identité Web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez la section Utilisateurs fédérés et rôles du Guide de l'utilisateur IAM.
  - Adhésion — Nimble Studio utilise un concept appelé « adhésion » pour permettre à un utilisateur d'accéder à un profil de lancement particulier. L'adhésion permet aux administrateurs de studio de déléguer l'accès aux ressources aux utilisateurs, sans avoir à rédiger ou à comprendre les politiques IAM. Lorsqu'un administrateur de Nimble Studio crée un abonnement pour un utilisateur dans un profil de lancement, celui-ci est autorisé à effectuer les actions IAM requises pour utiliser un profil de lancement, telles que la visualisation de ses propriétés et le démarrage d'une session de streaming à l'aide de ce profil de lancement.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Les rôles de service fournissent un accès uniquement à votre compte et ne peuvent pas être utilisés pour accorder l'accès aux services d'autres comptes. Un administrateur peut créer, modifier et supprimer un rôle de service depuis IAM. Pour plus d'informations, consultez la

section Création d'un rôle pour déléguer des autorisations à un Service AWS dans le guide de l'utilisateur IAM.

- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Nimble Studio ne prend pas en charge les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Pour savoir s'il faut utiliser des rôles ou des utilisateurs IAM, voir Quand créer un rôle IAM (au lieu d'un utilisateur) dans le guide de l'utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant aux identités ou aux AWS ressources IAM. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. Vous pouvez vous connecter en tant qu'utilisateur root ou en tant qu'utilisateur, ou vous pouvez assumer un rôle IAM. Lorsque vous faites ensuite une demande, AWS évalue les politiques associées basées sur l'identité ou les ressources. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez la section Présentation des politiques JSON dans le guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Chaque entité IAM (utilisateur ou rôle) démarre sans autorisation. En d'autres termes, par défaut, les utilisateurs ne peuvent rien faire, pas même changer leurs propres mots de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit associer une politique d'autorisations

à ce dernier. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent les actions que les utilisateurs et les rôles peuvent effectuer, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource à laquelle la politique est attachée, la stratégie définit les actions qu'un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Spécifiez un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs) dans Nimble Studio

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d’autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle). Vous pouvez définir une limite d’autorisations pour une entité. Les autorisations qui en résultent sont à l'intersection des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le `Principal` champ ne sont pas limitées par la limite des autorisations. Un refus explicite dans l’une de ces politiques annule l’autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les entités IAM dans le guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans Organizations. Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités des comptes membres, y compris pour chaque utilisateur Compte AWS root. Pour plus d'informations sur les Organizations SCPs, voir Comment SCPs travailler dans le Guide de AWS Organizations l'utilisateur.

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon Nimble Studio fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Nimble Studio, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Nimble Studio.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Nimble Studio

Fonctionnalité IAM	Assistance pour Nimble Studio
Actions politiques pour Nimble Studio	Oui
Ressources relatives aux politiques pour Nimble Studio	Oui
Clés de conditions de politique pour Nimble Studio	Oui
Listes de contrôle d'accès (ACLs) dans Nimble Studio	Non
Contrôle d'accès basé sur les attributs (ABAC) avec Nimble Studio	Oui

Fonctionnalité IAM	Assistance pour Nimble Studio
Utilisation d'informations d'identification temporaires avec Nimble Studio	Oui
Autorisations principales interservices pour Nimble Studio	Oui
Rôles de service pour Nimble Studio	Oui
Rôles liés à un service pour Nimble Studio	Non

Pour obtenir une vue d'ensemble de la façon dont Nimble Studio et les autres logiciels Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez le guide de l'Services AWS utilisateur d'IAM concernant leur compatibilité avec IAM.

Politiques basées sur l'identité pour Nimble Studio

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent les actions que les utilisateurs et les rôles peuvent effectuer, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques basées sur l'identité IAM, vous pouvez spécifier les actions et les ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur l'identité car il s'applique à l'utilisateur ou au rôle auquel il est attaché. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une politique JSON, consultez la référence des éléments de stratégie JSON IAM dans le guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Pour consulter des exemples de politiques basées sur l'identité de Nimble Studio, consultez. Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Politiques basées sur les ressources au sein de Nimble Studio

Prend en charge les politiques basées sur les ressources	Non

Nimble Studio ne prend pas en charge les politiques basées sur les ressources ni l'accès entre comptes. Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource à laquelle la politique est attachée, la stratégie définit les actions qu'un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Spécifiez un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Actions politiques pour Nimble Studio

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement pour lesquelles aucune opération d'API correspondante n'est associée. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de Nimble Studio, consultez la section Actions définies par Amazon Nimble Studio dans la référence d'autorisation de service.

Les actions politiques dans Nimble Studio utilisent le préfixe suivant avant l'action :

```
nimble
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité de Nimble Studio, consultez. Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Ressources relatives aux politiques pour Nimble Studio

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne prennent pas en charge les autorisations au niveau des ressources, telles que les opérations de listage, utilisez un caractère générique (*) pour indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter des exemples de politiques basées sur l'identité de Nimble Studio, consultez. Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Clés de conditions de politique pour Nimble Studio

Prend en charge les clés de condition de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Condition`élément (ou `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition` l'élément) est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations de la déclaration ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un utilisateur à accéder à une ressource uniquement si celle-ci est associée à son nom d'utilisateur. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour afficher toutes les clés de condition globales AWS , consultez Clés de contexte de condition globales AWS dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Nimble Studio, consultez. Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Listes de contrôle d'accès (ACLs) dans Nimble Studio

Supports ACLs	Non

Nimble Studio ne prend pas en charge les listes de contrôle d'accès (ACLs). ACLs contrôler les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Nimble Studio

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d’accès par attributs (ABAC) est une stratégie d’autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L’étiquetage des entités et des ressources est la première étape d’ABAC. Vous concevez ensuite des politiques ABAC pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Pour plus d'informations sur l'ABAC, voir Qu'est-ce que l'ABAC ? dans le guide de l'utilisateur IAM. Pour consulter un didacticiel présentant les étapes de configuration d'ABAC, consultez la section Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Nimble Studio

Prend en charge les informations d’identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par

exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passer à un rôle (console) dans le guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Nimble Studio

Prend en charge les autorisations de principal	Oui

Rôles de service pour Nimble Studio

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Les rôles de service fournissent un accès uniquement à votre compte et ne peuvent pas être utilisés pour accorder l'accès aux services d'autres comptes. Un administrateur peut créer, modifier et supprimer un rôle de service depuis IAM. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un Service AWS dans le guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de Nimble Studio. Modifiez les rôles de service uniquement lorsque Nimble Studio fournit des instructions à cet effet.

Rôles liés à un service pour Nimble Studio

Prend en charge les rôles liés à un service	Non

Nimble Studio ne prend pas en charge les rôles liés à un service. Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s’affichent dans votre compte IAM et sont la propriété du service. Un administrateur peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion de rôles liés à un service, consultez la section relative à l'Services AWS utilisation d'IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon Nimble Studio

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Nimble Studio. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur doit créer des politiques IAM qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des actions sur les ressources dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes ayant besoin de ces autorisations.

Pour savoir comment créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, consultez la section Création de politiques dans l'onglet JSON du guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité sont très puissantes. Ils déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Nimble Studio dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l’identité, suivez ces instructions et recommandations :

- Commencez à utiliser des politiques AWS gérées — Pour commencer à utiliser Nimble Studio rapidement, utilisez des politiques AWS gérées pour donner à vos employés les autorisations dont ils ont besoin. Ces politiques sont déjà disponibles dans votre compte et sont gérées et mises à jour par AWS. Pour plus d'informations, voir Commencer à utiliser les autorisations avec les politiques AWS gérées dans le Guide de l'utilisateur IAM.
- Accorder le moindre privilège : lorsque vous créez des politiques personnalisées, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Commencez avec un ensemble d'autorisations minimum et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard. Pour plus d'informations, consultez Accorder le moindre privilège possible dans le Guide de l'utilisateur IAM.
- Activez l'authentification multifactorielle pour les opérations sensibles : pour plus de sécurité, demandez aux utilisateurs d'utiliser l'authentification multifactorielle (MFA) pour accéder aux ressources sensibles ou aux opérations d'API. Pour plus d'informations, consultez la section Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'utilisateur IAM.
- Utilisez des conditions de politique pour renforcer la sécurité : dans la mesure du possible, définissez les conditions dans lesquelles vos politiques basées sur l'identité autorisent l'accès à une ressource. Par exemple, vous pouvez rédiger les conditions pour spécifier une plage d'adresses IP autorisées d'où peut provenir une demande. Vous pouvez également écrire des conditions pour autoriser les requêtes uniquement à une date ou dans une plage de temps spécifiée, ou pour imposer l'utilisation de SSL ou de MFA. Pour plus d'informations, voir Éléments de politique IAM JSON : Condition dans le guide de l'utilisateur IAM.

AWS politiques gérées pour Amazon Nimble Studio

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l’expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d’utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités.

Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Quand un service lance une nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

Vos utilisateurs finaux accèderont principalement à Amazon Nimble Studio via le portail Nimble Studio. Lorsque vous créez votre studio à l'aide StudioBuilder de la console Nimble Studio, un rôle IAM est créé pour chaque personnage du studio : l'administrateur du studio et l'utilisateur du studio. Chacun est associé à la politique gérée IAM correspondante. Le portail Nimble Studio offre une expérience dans laquelle les utilisateurs peuvent uniquement répertorier et utiliser les ressources auxquelles ils sont autorisés à accéder.

Le portail Nimble Studio offre une expérience dans laquelle les utilisateurs peuvent uniquement répertorier et utiliser les ressources auxquelles ils ont accès. Le portail dépend du contenu de ces politiques pour fonctionner correctement. Les utilisateurs finaux de Nimble Studio utiliseront le portail pour accéder à leur studio cloud. Ainsi, lorsque les administrateurs créent leur studio en utilisant StudioBuilder, un rôle IAM est créé pour chaque personne devant accéder au studio. Cela inclut l'administrateur du studio et l'utilisateur du studio, chacun étant associé à sa politique gérée IAM respective.

Pour obtenir une liste et une description des politiques relatives aux fonctions de travail, voir les politiques AWS gérées pour les fonctions de travail dans le guide de l'utilisateur d'IAM.

AWS politique gérée : `AmazonNimbleStudio-LaunchProfileWorker`

Vous pouvez associer la politique `AmazonNimbleStudio-LaunchProfileWorker` à vos identités IAM.

Associez cette politique aux EC2 instances créées par Nimble Studio Builder pour accorder l'accès aux ressources nécessaires aux responsables du profil de lancement de Nimble Studio.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- ds - Permet aux LaunchProfile travailleurs de découvrir les informations de connexion concernant les informations AWS Managed Microsoft AD associées à un LaunchProfile.
- ec2 - Permet aux utilisateurs de LaunchProfile découvrir les informations sur les groupes de sécurité et les sous-réseaux pour se connecter à un. LaunchProfile
- fsx - Permet aux LaunchProfile utilisateurs de découvrir les informations de connexion aux FSx volumes Amazon associés à un LaunchProfile.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

AWS politique gérée : **AmazonNimbleStudio-StudioAdmin**

Vous pouvez associer la politique AmazonNimbleStudio-StudioAdmin à vos identités IAM.

Associez cette politique au rôle d'administrateur associé à votre studio pour accorder l'accès aux ressources Amazon Nimble Studio associées à l'administrateur du studio et aux ressources de studio associées dans d'autres services.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- nimble - Permet aux utilisateurs de Studio d'accéder aux ressources Nimble qui leur ont été déléguées par. StudioAdmins
- sso - Permet aux utilisateurs du studio de voir les noms des autres utilisateurs du studio.
- identitystore - Permet aux utilisateurs du studio de voir les noms des autres utilisateurs du studio.
- ds - Permet à Nimble Studio d'ajouter des postes de travail virtuels à ceux AWS Managed Microsoft AD associés au studio.
- ec2 - Permet à Nimble Studio d'associer des postes de travail virtuels à votre VPC configuré.
- fsx - Permet à Nimble Studio de connecter des postes de travail virtuels à vos volumes Amazon configurés. FSx
- cloudwatch - Permet à Nimble Studio de récupérer CloudWatch des métriques.

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
```

```
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
```

```
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS politique gérée : **AmazonNimbleStudio-StudioUser**

Vous pouvez associer la politique AmazonNimbleStudio-StudioUser à vos identités IAM.

Associez cette politique au rôle d'utilisateur associé à votre studio pour accorder l'accès aux ressources Amazon Nimble Studio associées à l'utilisateur du studio et aux ressources de studio associées dans d'autres services.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- nimble - Permet aux utilisateurs de Studio d'accéder aux ressources Nimble qui leur ont été déléguées par. StudioAdmins
- sso - Permet aux utilisateurs du studio de voir les noms des autres utilisateurs du studio.
- identitystore - Permet aux utilisateurs du studio de voir les noms des autres utilisateurs du studio.
- ds - Permet à Nimble Studio d'ajouter des postes de travail virtuels à ceux AWS Managed Microsoft AD associés au studio.
- ec2 - Permet à Nimble Studio d'associer des postes de travail virtuels à votre VPC configuré.
- fsx - Permet à Nimble Studio de connecter des postes de travail virtuels à vos volumes Amazon configurés. FSx

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

Mises à jour des politiques AWS gérées par Nimble Studio

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon Nimble Studio depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
AWS politique gérée : AmazonNimbleStudio-StudioUser – Mise à jour de politique	Amazon Nimble Studio a mis à jour une politique visant à utiliser la dernière version du service Identity Store.	22 septembre 2023
AWS politique gérée : AmazonNimbleStudio-StudioAdmin – Mise à jour de politique	Amazon Nimble Studio a mis à jour une politique visant à utiliser la dernière version du service Identity Store.	22 septembre 2023
AWS politique gérée : AmazonNimbleStudio-StudioUser – Mise à jour de politique	Amazon Nimble Studio a mis à jour une politique permettant aux utilisateurs du studio de consulter les sauvegardes de leurs postes de travail.	20 décembre 2022
AWS politique gérée : AmazonNimbleStudio-StudioAdmin – Mise à jour de politique	Amazon Nimble Studio a mis à jour la politique afin de permettre aux administrateurs du studio de consulter les sauvegardes de leurs postes de travail.	20 décembre 2022
AWS politique gérée : AmazonNimbleStudio-StudioUser – Mise à jour de politique	Amazon Nimble Studio a mis à jour une politique permettant aux administrateurs du studio de récupérer CloudWatch des statistiques.	11 novembre 2021
AWS politique gérée : AmazonNimbleStudio-	Amazon Nimble Studio a mis à jour la politique afin de	1er novembre 2021

Modification	Description	Date
`StudioUser` – Mise à jour de politique	permettre aux utilisateurs du studio de démarrer et d'arrêter leurs postes de travail.	
AWS politique gérée : `AmazonNimbleStudio-StudioAdmin` – Mise à jour de politique	Amazon Nimble Studio a mis à jour la politique afin de permettre aux administr ateurs de studio de démarrer et d'arrêter leurs postes de travail.	1er novembre 2021
AWS politique gérée : `AmazonNimbleStudio-StudioUser` – Mise à jour de politique	Amazon Nimble Studio a mis à jour la politique afin d'autoriser de manière conditionnelle l'accès aux ressources des sessions de streaming en fonction de. `nimble:ownedBy` `nimble:createdBy`	16 août 2021
AWS politique gérée : `AmazonNimbleStudio-StudioUser` : nouvelle politique	Amazon Nimble Studio a ajouté une nouvelle politique qui autorise l'accès aux ressources associées à l'utilisateur du studio et aux ressources de studio associées dans d'autres services.	28 avril 2021

Modification	Description	Date
AWS politique gérée : `AmazonNimbleStudio-StudioAdmin` : nouvelle politique	Amazon Nimble Studio a ajouté une nouvelle politique qui autorise l'accès aux ressources associées à l'administrateur du studio et aux ressources de studio associées dans d'autres services.	28 avril 2021
AWS politique gérée : `AmazonNimbleStudio-LaunchProfileWorker` : nouvelle politique	Amazon Nimble Studio a ajouté une nouvelle politique qui permet d'accéder aux ressources nécessaires aux responsables du profil de lancement de Nimble Studio.	28 avril 2021
Amazon Nimble Studio a commencé à suivre les modifications	Amazon Nimble Studio a commencé à suivre les modifications apportées à ses politiques AWS gérées.	28 avril 2021

Prévention du problème de l’adjoint confus entre services

Le problème des adjoints confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à effectuer l'action. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L’usurpation d’identité entre services peut se produire lorsqu’un service (le service appelant) appelle un autre service (le service appelé). Le service d'appel peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client d'une manière à laquelle il ne devrait pas être autorisé à accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition `aws:SourceAccount` globale `aws:SourceArn` et les clés contextuelles dans les politiques de ressources afin de limiter les

autorisations accordées par Identity and Access Management (IAM) à Amazon Nimble Studio pour accéder à vos ressources. Si vous utilisez les deux clés contextuelles de condition globale, la `aws:SourceAccount` valeur et le compte figurant dans la `aws:SourceArn` valeur doivent utiliser le même identifiant de compte lorsqu'ils sont utilisés dans la même déclaration de politique.

La valeur de `aws:SourceArn` doit être l'ARN du studio et `aws:SourceAccount` doit être votre identifiant de compte. Vous ne saurez pas quel est l'identifiant du studio tant que celui-ci n'est pas créé, car il est généré par Nimble Studio. Une fois votre studio créé, vous pouvez mettre à jour la politique de confiance en définissant l'identifiant final du studio comme étant le`aws:SourceArn`.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de condition de contexte `aws:SourceArn` global avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:nimble::123456789012:*`.

Vos utilisateurs finaux assument votre rôle de studio lorsqu'ils se connectent au portail Nimble Studio. Lorsque vous créez votre studio, AWS configurez le rôle et évaluez la politique. AWS évalue la politique chaque fois qu'un de vos utilisateurs se connecte au portail Nimble Studio. Lorsque vous créez un studio, vous ne pouvez pas modifier le`aws:SourceArn`. Une fois que vous avez fini de créer votre studio, vous pouvez utiliser votre StudioArn pour le. `aws:SourceArn`

L'exemple suivant est une politique d'acceptation des rôles qui montre comment utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans Nimble Studio pour éviter le problème de confusion des adjoints.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

Résolution des problèmes d'identité et d'accès à Amazon Nimble Studio

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Nimble Studio et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Nimble Studio.
- Je ne suis pas autorisé à exécuter iam :PassRole.
- Je veux afficher mes clés d’accès
- Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Nimble Studio.
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources Nimble Studio.

Je ne suis pas autorisé à effectuer une action dans Nimble Studio.

Si vous recevez une erreur qui indique que vous n’êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d’effectuer l’action.

L’exemple d’erreur suivant se produit quand l’utilisateur IAM `mateojackson` tente d’utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `nimble:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 nimble:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s’applique à l’utilisateur `mateojackson` doit être mise à jour pour autoriser l’accès à la ressource *`my-example-widget`* à l’aide de l’action `nimble:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter iam :PassRole.

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, contactez votre administrateur pour obtenir de l'aide. Demandez-leur de mettre à jour vos politiques afin de vous permettre de transférer un rôle à Nimble Studio.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service, au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur nommé `johndoe` essaie d'utiliser la console pour effectuer une action dans Nimble Studio. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du service. John n'est pas autorisé à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/johndoe is not authorized to perform: iam:PassRole
```

Dans ce cas, John demande à son administrateur de mettre à jour ses politiques pour autoriser l'exécution de l'`iam:PassRole`action.

Je veux afficher mes clés d'accès

Amazon Nimble Studio ne fournit pas de clés d'accès. Pour en savoir plus sur les clés d'accès secrètes, consultez la section Gestion des clés d'accès dans le guide de l'utilisateur IAM.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour vous aider à trouver votre nom d'utilisateur canonique. En effet, vous lui accorderiez ainsi un accès permanent à votre compte.

Lorsque vous créez une paire de clés d'accès, vous êtes invité à enregistrer l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, ajoutez de nouvelles clés d'accès à votre utilisateur. Vous pouvez avoir un maximum de deux clés d'accès. Si

vous en avez déjà deux, supprimez une paire de clés avant d'en créer une nouvelle. Pour consulter les instructions, reportez-vous à la section Gestion des clés d'accès dans le guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder à Nimble Studio.

Pour autoriser d'autres personnes à accéder à Nimble Studio, créez une entité IAM (utilisateur ou rôle) pour la personne ou l'application qui a besoin d'y accéder. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Attachez ensuite une politique à l'entité qui lui accorde les autorisations appropriées.

Nimble Studio vous fournit `AmazonNimbleStudio-StudioUser` le AWS Management Console. L'administrateur informatique qui gère la console utilise cette politique pour accorder l'accès au studio à d'autres personnes.

Pour un didacticiel sur l'utilisation de la politique d'administration, consultez le Configuration de Nimble Studio guide. Pour savoir comment associer des politiques existantes aux utilisateurs, telles que les politiques relatives aux utilisateurs et aux profils de lancement, consultez la section Création d'utilisateurs IAM (console).

Pour plus d'informations sur l'importation de politiques, consultez la section Création de votre premier utilisateur délégué et de votre premier groupe IAM dans le Guide de l'utilisateur IAM.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources Nimble Studio.

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Nimble Studio prend en charge ces fonctionnalités, consultezComment Amazon Nimble Studio fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les rôles IAM diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Enregistrement et surveillance des événements de sécurité avec Nimble Studio

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Nimble Studio et de vos AWS solutions. Collectez des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant.

AWS et Nimble Studio fournissent des outils pour surveiller vos ressources et répondre aux incidents potentiels, notamment un guide Enregistrement des appels Nimble Studio à l'aide de AWS CloudTrail de AWS CloudFormation l'utilisateur.

Pour plus d'informations sur le fonctionnement d'Amazon Nimble Studio AWS CloudFormation, notamment des exemples de modèles JSON et YAML, consultez la référence aux ressources et aux propriétés Amazon Nimble Studio dans le guide de l' AWS CloudFormation utilisateur. Pour comprendre comment utiliser les CloudFormation modèles, reportez-vous à la section AWS CloudFormation Concepts.

Rubriques

- Enregistrement des appels Nimble Studio à l'aide de AWS CloudTrail

Enregistrement des appels Nimble Studio à l'aide de AWS CloudTrail

Amazon Nimble Studio est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS dans Nimble Studio. CloudTrail capture tous les appels d'API pour Nimble Studio sous forme d'événements. Les appels capturés

incluent des appels provenant de la console Nimble Studio et des appels de code vers les opérations Amazon Nimble Studio.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Nimble Studio. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Nimble Studio, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Informations sur Nimble Studio dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Nimble Studio, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris ceux de Nimble Studio, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d’activité dans la console, il s’applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence.

Pour plus d’informations, consultez les ressources suivantes :

Présentation de la création d’un journal de suivi

CloudTrail services et intégrations pris en charge

Configuration des notifications Amazon SNS pour CloudTrail

Réception de fichiers CloudTrail journaux provenant de plusieurs régions

Réception de fichiers CloudTrail journaux provenant de plusieurs comptes

Les actions de Nimble Studio sont enregistrées CloudTrail et documentées dans le manuel Amazon Nimble Studio API Reference. Par exemple, les appels au CreateStudio GetStudio et les DeleteStudio actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service .

Pour plus d'informations, consultez l'élément Identité de l'CloudTrail utilisateur.

Comprendre les entrées du fichier journal de Nimble Studio

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, sur tous les paramètres, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne sont pas des séries ordonnées retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

Cet exemple JSON montre trois actions :

- ACTION_1 : CreateStudio
- ACTION 2 : GetStudio
- ACTION_3 : DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
```

```
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
```

```
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

Dans l'exemple, vous remarquerez que les événements indiquent la région, l'adresse IP et d'autres « RequestParameters » tels que les « » et userRoleArn « adminRoleArn » qui vous aideront à identifier l'événement. Vous pouvez voir l'heure et la date dans le champ « CreationDate », ainsi que la source d'origine de la demande, marquée comme « EventSource » : « nimble.amazonaws.com ».

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans IAM ou AWS STS, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS.

AWS CloudTrail capture tous les appels d'API pour IAM et AWS Security Token Service (AWS STS) sous forme d'événements, y compris les appels depuis la console et les appels d'API. Pour en savoir plus sur l'utilisation CloudTrail avec IAM et AWS STS, consultez la section Journalisation des appels IAM et AWS STS API avec. AWS CloudTrail

Pour plus d'informations CloudTrail, consultez le Guide de AWS CloudTrail l'utilisateur.

Pour plus d'informations sur les autres services de surveillance proposés par Amazon, consultez le guide de CloudWatch l'utilisateur Amazon.

Validation de conformité pour Amazon Nimble Studio

Amazon Nimble Studio suit le modèle de responsabilité partagée, et la conformité est partagée entre AWS et nos clients.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et

réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Sécurité de l'infrastructure dans Amazon Nimble Studio

En tant que service géré, Amazon Nimble Studio est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Nimble Studio via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Bonnes pratiques de sécurité pour Nimble Studio

Amazon Nimble Studio fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de Nimble Studio et de vos AWS solutions. Pour plus d'informations sur la surveillance et la réponse aux événements, consultezEnregistrement et surveillance des événements de sécurité avec Nimble Studio.

Protection des données

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une CLI ou une API, utilisez un point de terminaison FIPS. Pour de plus amples informations sur les points de terminaison FIPS disponibles, consultez Federal Information Processing Standard (FIPS) 140-2.

Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Name (Nom). Cela inclut lorsque vous travaillez avec Amazon Nimble Studio ou autre à Services AWS l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous saisissez dans Amazon Nimble Studio ou dans d'autres services peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Autorisations

Gérez l'accès aux AWS ressources à l'aide des utilisateurs, des rôles IAM et en accordant le moindre privilège aux utilisateurs. Établissez des politiques et des procédures de gestion des informations d'identification pour la création, la distribution, la rotation et la révocation des informations AWS d'accès. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Support pour Nimble Studio

Cette section fournit des options de support pour Nimble Studio, notamment comment obtenir de l'aide lors du déploiement ou de l'utilisation du service et de ses applications associées.

Table des matières

Forum Nimble Studio

Si vous avez des questions sur Nimble Studio, vous pouvez consulter le forum Nimble Studio. Vous pouvez y obtenir des réponses de la part de la communauté et des modérateurs AWS du forum sur les fonctionnalités de Nimble Studio, les problèmes techniques et l'aide au dépannage.

Support des applications

Nimble Studio fournit de la documentation supplémentaire pour les applications suivantes.

AWSThinkboxDeadline

Pour obtenir de l'aide concernant votre ferme de rendu ou pour savoir comment Deadline fonctionne, voir AWSThinkboxDeadline documentation.

Studio agile File Transfer

Pour savoir comment fonctionne le transfert de fichiers, consultez le guide de l'utilisateur de Nimble Studio File Transfer.

Support Centre

Le Support Centre est une plateforme dédiée à la création et à la gestion de vos dossiers d'assistance. Il donne accès à diverses ressources, notamment des solutions techniques et de

facturation, un centre de connaissances, des vidéos du centre de connaissances, de AWS la documentation, ainsi que des formations et des certifications.

Support plans

Support les plans vous aident à optimiser les performances, à garantir la sécurité, à éviter les temps d'arrêt et à contrôler les coûts. Pour plus d'informations sur Support les forfaits, voir Comparer les Support forfaits.

Pour plus d'informations sur la manière dont nous AWS pouvons vous aider, consultez la page Contactez-nous.

Historique du document

- Version de l'API : dernière en date
- Dernière mise à jour de la documentation : 2 octobre 2024

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l'administrateur de Nimble Studio.

Modification	Description	
Avis de fin de support	Avis de fin de support : le 22 octobre 2024, le support d'Amazon Nimble Studio AWS sera interrompu. Après le 22 octobre 2024, vous ne pourrez plus accéder à la console Nimble Studio ni aux ressources de Nimble Studio.	2 octobre 2024
AWS mises à jour des politiques gérées	Mise à jour `AmazonNimbleStudio-StudioAdmin` des politiques `AmazonNimbleStudio-StudioUser` et pour utiliser la dernière version du AWS IAM Identity Center service.	22 septembre 2023
Nouveau guide et service	Il s'agit de la version initiale d'Amazon Nimble Studio et du guide de l'administrateur d'Amazon Nimble Studio.	19 juin 2023

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.