aws

Guide de l'administrateur

AWS Supply Chain

AWS Supply Chain: Guide de l'administrateur

Table of Contents

Qu'est-ce que AWS Supply Chain ?

AWS Supply Chainest une application de gestion de la chaîne d'approvisionnement basée sur le cloud qui fonctionne avec vos solutions existantes telles que les systèmes de planification des ressources d'entreprise (ERP) et de gestion de la chaîne d'approvisionnement. Vous pouvez ainsi connecter et extraire vos données relatives à l'inventaire, à l'approvisionnement et à la demande à partir de systèmes ERP ou de chaîne d'approvisionnement existants dans un modèle deAWS Supply Chain données unifié.AWS Supply Chain

Rubriques

Navigateurs web pris en charge par AWS Supply Chain

Avant de travailler avecAWS Supply Chain, vérifiez que votre navigateur est compatible à l'aide du tableau suivant.

Navigateur	Versions prises en charge
Google Chrome	Trois versions les plus récentes.
Mozilla Firefox ESR	Les versions sont prises en charge jusqu'à leur end-of-lifedate de mise à jour dans Firefox. Pour plus de détails, consultez le calendrier des versions de Firefox ESR.
Mozilla Firefox	Trois versions les plus récentes.
Microsoft Edge et Edge Chromium	Version 84 et versions ultérieures.
Safari	Safari 10 ou version ultérieure sur macOS.

Langues prises en charge parAWS Supply Chain

AWS Supply Chain prend en charge les langues suivantes :

- Anglais (États-Unis)
- Anglais (Royaume-Uni)
- Allemand
- Espagnol
- Français
- Italien
- Portugais
- Chinois (simplifié)
- Chinois (traditionnel)
- Japonais
- Coréen
- Indonésien

Création d'un AWS compte

Utilisez cette section pour créer un AWS compte et créer un utilisateur IAM. Pour plus d'informations sur les meilleures pratiques relatives à la création d'un AWS compte, consultez la section Création de votre AWS environnement de bonnes pratiques.

Rubriques

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 https://portal.aws.amazon.com/billing/signup.
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 en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

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

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, 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, accordez 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.

Connectez-vous en tant qu'utilisateur disposant 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.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Fermeture d'un AWS compte

Pour plus d'informations sur la procédure à suivre pour fermer un AWS compte, consultez la section Fermeture d'un compte.

Commencer avec AWS Supply Chain

Dans cette section, vous apprendrez à créer une AWS Supply Chain instance, à octroyer des rôles d'autorisation aux utilisateurs, à vous connecter à l'application AWS Supply Chain Web et à créer des rôles d'autorisation utilisateur personnalisés. An Compte AWS peut avoir jusqu'à 10 AWS Supply Chain instances en état actif ou en cours d'initialisation.

Rubriques

Prérequis

Avant de créer une AWS Supply Chain instance, assurez-vous de suivre les étapes suivantes :

- Vous avez créé un Compte AWS. Pour plus d’informations, consultez Création d'un AWS compte.

> **Note**
>
> Si vous ne l'avez pas encore activé AWS IAM Identity Center, créez une AWS organisation et activez IAM Identity Center. Pour plus d'informations sur la création d'une AWS organisation, voir Création d'une organisation.

- Activez IAM Identity Center à l' Région AWS endroit où vous souhaitez créer votre AWS Supply Chain instance. AWS Supply Chain est uniquement pris en charge dans les régions USA Est (Virginie du Nord), USA Ouest (Oregon), Europe (Francfort) et Europe (Irlande). Pour plus d'informations, consultez Activation du centre d'identité IAM .

> **Note**
>
> AWS Supply Chain La planification de la demande et la planification de l'approvisionnement ne sont pas prises en charge dans la région Europe (Irlande).

> **Note**
>
> Si vous n'avez pas activé le centre d'identité IAM dans une région autre que celles répertoriées ici, vous ne pouvez pas créer d' AWS Supply Chain instance.

- Vous pouvez créer des utilisateurs IAM à partir de la console AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Création d'un AWS compte.
- Ajoutez les utilisateurs qui ont besoin d'accéder AWS Supply Chain à IAM Identity Center. Pour plus d'informations, consultez Ajouter des utilisateurs dans IAM Identity Center. Vous pouvez également connecter votre Active Directory à IAM Identity Center. Pour plus d'informations, voir Se connecter à un annuaire Microsoft AD dans le Guide de AWS IAM Identity Center l'utilisateur.
- Lorsque vous utilisez Microsoft Active Directory, assurez-vous que la synchronisation Active Directory est activée.
- Vous devez AWS Key Management Service (AWS KMS) pour créer une instance. AWS Supply Chain l'utilise AWS KMS key pour crypter toutes les données qui entrent. AWS Supply Chain

Utilisation de la console AWS Supply Chain

> **Note**
>
> Si votre AWS compte est un compte membre d'une AWS organisation et inclut une politique de contrôle des services (SCP), assurez-vous que le SCP de l'organisation accorde les autorisations suivantes au compte membre. Si les autorisations suivantes ne sont pas

incluses dans la politique SCP de l'organisation, la création de l' AWS Supply Chain instance échouera.

Pour accéder à la AWS Supply Chain console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS Supply Chain des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la AWS Supply Chain console, associez également la politique AWS Supply Chain `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

L'administrateur de la console a besoin des autorisations suivantes pour créer et mettre à jour AWS Supply Chain des instances avec succès.

```
        {
"Version": "2012-10-17",
"Statement": [
    {
        "Action": "scn:*",
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:ListBucket",
            "s3:CreateBucket",
            "s3:PutBucketVersioning",
            "s3:PutBucketObjectLockConfiguration",
            "s3:PutEncryptionConfiguration",
            "s3:PutBucketPolicy",
```

```
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketNotification",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketLogging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::aws-supply-chain-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "chime:CreateAppInstance",
                "chime:DeleteAppInstance",
                "chime:PutAppInstanceRetentionSettings",
                "chime:TagResource"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
```

```
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
```

```
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Création d'une instance

> **Note**
>
> Vous pouvez créer jusqu'à 10 instances dans un Compte AWS. Les 10 instances incluent des instances actives et en cours d'initialisation. Si vous avez déjà activé IAM Identity Center (successeur de AWS Single Sign-On), vous devez créer votre AWS Supply Chain instance Région AWS là où vous avez activé IAM Identity Center. AWS Supply Chain ne prend pas en charge les appels IAM Identity Center entre les régions.

Pour créer une AWS Supply Chain instance, procédez comme suit.

> **Note**
>
> Seul l' AWS Management Console administrateur peut créer une instance. L' AWS Management Console administrateur qui crée l' AWS Supply Chain instance doit disposer de

toutes les autorisations répertoriées ci-dessousUtilisation de la console AWS Supply Chain. Cet administrateur doit inviter un utilisateur IAM en tant qu' AWS Supply Chain administrateur pour gérer AWS Supply Chain.

1. Ouvrez la AWS Supply Chain console à l'adressehttps://console.aws.amazon.com/scn/home.
2. Si nécessaire, changez la Région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le guide de l'utilisateur IAM. Consultez également la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

   > **Note**
   >
   > AWS Supply Chain n'est pris en charge que dans les régions USA Est (Virginie du Nord), USA Ouest (Oregon), Europe (Francfort), Asie-Pacifique (Sydney) et Europe (Irlande). AWS Supply Chain La planification de la demande et la planification de l'approvisionnement ne sont pas prises en charge dans la région Europe (Irlande).

3. Sur le AWS Supply Chain tableau de bord, choisissez Create instance.
4. Sur la page des propriétés de l'instance, entrez les informations suivantes :

   - AWS Région — Choisissez la région dans laquelle vous avez activé IAM Identity Center. Pour changer de région, choisissez Sélectionner une région dans le menu déroulant en haut à droite. Vous ne pouvez pas modifier la région après avoir créé l'instance.
   - Nom — Entrez le nom de l'instance.
   - (Facultatif) Description — Entrez une description pour l'instance.

5. Sous CléAWS KMS, entrez votre clé KMS et mettez à jour votre politique en matière de clé KMS comme suit :

   > **Note**
   >
   > En tant qu'administrateur d'application, lorsque vous ajoutez des utilisateurs à l' AWS Supply Chain instance, ils ont accès au AWS KMS key. Vous pouvez gérer les autorisations des utilisateurs pour ajouter ou supprimer des utilisateurs. Pour plus

d'informations sur les autorisations des utilisateurs, consultezRôles d'autorisation utilisateur.

> **Note**
>
> Remplacez *la région* *YourAccountNumber*, l'*YourInstanceID* et *YourKmsKeyArn*par votre AWS région Compte AWS, l'ID d' AWS Supply Chain instance et la AWS KMS clé.

```
   {
   "Version": "2012-10-17",
   "Statement": [{
           "Sid": "Enable IAM User Permissions",
           "Effect": "Allow",
           "Principal": {
               "AWS": "arn:aws:iam::YourAccountNumber:root"
           },
           "Action": "kms:*",
           "Resource": "*"
       },
       {
           "Sid": "Allow access through SecretManager for all principals in the
account that are authorized to use SecretManager",
           "Effect": "Allow",
           "Principal": {
               "AWS": "*"
           },
           "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
               "kms:ReEncrypt*",
               "kms:GenerateDataKey*",
               "kms:CreateGrant",
               "kms:DescribeKey",
               "kms:GenerateDataKeyWithoutPlaintext",
               "kms:ReEncryptFrom",
               "kms:ReEncryptTo"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }

            }
        }
    ]
}
```

Si vous n'avez pas de clé KMS, choisissez Create pour accéder à la AWS KMS console, où vous pouvez créer cette clé. Utilisez la politique de clé KMS précédente. Pour obtenir des informations détaillées sur la création de clés KMS, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

Si vous prévoyez d'utiliser une connexion de données S/4 Hana, assurez-vous que la clé KMS que vous avez fournie possède la aws-supply-chain-accessbalise associée à une valeur vraie.

6. (Facultatif) Sous Balises d'instance, choisissez Ajouter une nouvelle balise pour attribuer une balise à votre instance. Vous pouvez utiliser ces balises pour identifier votre instance. Pour plus d'informations sur les balises, consultez la section Création de balises.
7. Choisissez Créer une instance.

   La création de l' AWS Supply Chain instance prend environ 2 à 3 minutes. Une fois l'instance créée, le champ Status du AWS Supply Chain tableau de bord s'affiche comme Actif.
8. Une fois votre AWS Supply Chain instance créée, mettez à jour votre politique KMS pour autoriser AWS Supply Chain l'accès à votre AWS KMS clé.

> **Note**
>
> Remplacez *YourInstancel'ID* par l'ID de votre AWS Supply Chain instance. Vous trouverez l'ID de votre instance sur le tableau de bord de la AWS Supply Chain console.

```
        {
```

```
    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "scn.Region.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource":"YourKmsKeyArn"
}
```

Activation du centre d'identité IAM

Avant de commencer à l'utiliser AWS Supply Chain, vous devez vous connecter à une source d'identité. Pour plus d'informations, consultez la section Getting started with IAM dans le guide de l'utilisateur d'IAM.

Ajouter des utilisateurs dans IAM Identity Center

Vous pouvez gérer les utilisateurs pour qu' AWS Supply Chain ils utilisent le service IAM Identity Center. IAM Identity Center est un service IAM Identity Center basé sur le cloud qui facilite la gestion centralisée de l'accès IAM Identity Center à toutes vos applications Comptes AWS et à celles du cloud. Pour ajouter des utilisateurs IAM, consultez la section Création d'un utilisateur IAM dans votre compte AWS dans le guide de l'utilisateur IAM.

Pour plus d'informations sur la création de groupes d'utilisateurs IAM, consultez la section Création de groupes d'utilisateurs IAM dans le Guide de l'utilisateur IAM.

> **Note**
>
> Pour ajouter un utilisateur AWS Supply Chain, celui-ci doit faire partie d'un groupe IAM Identity Center.

Choix du propriétaire de AWS Supply Chain l'application

> **Note**
>
> En tant qu'administrateur de AWS console, vous choisissez le propriétaire de AWS Supply Chain l'application pour gérer l'accès aux applications AWS Supply Chain Web. Le propriétaire de AWS Supply Chain l'application peut ajouter ou supprimer des rôles d'autorisation utilisateur dans l'application AWS Supply Chain Web.

Une fois l'instance créée et une source d'identité connectée, procédez comme suit pour choisir le propriétaire de AWS Supply Chain l'application.

1. Sur le tableau de bord de la AWS Supply Chain console, sous Propriétaire de l'application, choisissez Attribuer le propriétaire de l'application.
2. Sous Sélectionner le propriétaire de l'application, sélectionnez un utilisateur qui agira en tant que propriétaire de AWS Supply Chain l'application. Vous ne pouvez rechercher que le nom d'utilisateur et les utilisateurs correspondant aux critères de recherche apparaissent.

Pour ajouter d'autres utilisateurs, choisissez Go to IAM Identity Center. Pour plus d'informations sur l'ajout d'utilisateurs, voir Ajouter des utilisateurs dans IAM Identity Center et pour plus d'informations sur les rôles d'autorisation des utilisateurs, voirRôles d'autorisation utilisateur.

> **Note**
>
> Vous ne pouvez ajouter qu'un seul utilisateur à la fois depuis la AWS Supply Chain console. Vous ne pouvez pas ajouter de groupe en tant que propriétaire d'une application AWS Supply Chain.

3. choisissez Envoyer une invitation.

   Sur le tableau de bord de la AWS Supply Chain console, vous verrez l'utilisateur répertorié sous Propriétaire de l'application.

4. Choisissez Gérer AWS Supply Chain pour ajouter et supprimer des utilisateurs dans l'application AWS Supply Chain Web.

Attribuer des groupes

En tant que propriétaire ou AWS Supply Chain administrateur d'une application, vous ne pouvez ajouter que des utilisateurs faisant partie d'un groupe IAM Identity Center à AWS Supply Chain.

1. Sur le tableau de bord de la AWS Supply Chain console, sous Groupes, choisissez Attribuer des groupes.

   La page Groupes s'affiche.

2. Sous Nom du groupe, sélectionnez le groupe auquel les utilisateurs peuvent accéder AWS Supply Chain et choisissez Attribuer.

   Vous verrez le groupe que vous avez répertorié sous Groupes dans le AWS Supply Chain tableau de bord.

3. Vous pouvez choisir Gérer les groupes pour ajouter un nouveau groupe dans IAM Identity Center. Une fois le groupe ajouté dans IAM Identity Center, il sera répertorié sous Nom du groupe dans AWS Supply Chain.

Connexion à l'application Web de chaîne d' AWS approvisionnement

En tant qu' AWS Supply Chain administrateur, vous devriez avoir reçu un e-mail d'invitation à accéder à l'application AWS Supply Chain Web.

1. Vous pouvez choisir le lien dans l'e-mail ou sur le tableau de bord de la AWS Supply Chain console, sous Sous-domaine, choisissez l'URL Web.

   La page de connexion à l'application AWS Supply ChainWeb apparaît.
2. Entrez les informations d'identification de l'utilisateur AWS IAM Identity Center et choisissez Se connecter.

Connexion AWS Supply Chain pour la première fois

> **Note**
>
> Il ne vous sera demandé de compléter les profils de votre compte et de votre organisation que lorsque vous vous connecterez pour la première fois.

Après vous être connecté à l'application AWS Supply Chain Web en tant AWS Supply Chain qu'administrateur, procédez comme suit pour terminer la configuration.

1. Sur la page Complétez votre profil, saisissez le titre de votre poste et votre fuseau horaire. Choisissez Suivant.
2. Sur la page Ajoutons les informations de votre organisation, entrez le nom de l'organisation et choisissez l'emplacement du siège social. Vous pouvez éventuellement ajouter un logo d'entreprise. Choisissez Suivant.
3. Sur la AWS Supply Chain page Configurer vos coéquipiers, sélectionnez les utilisateurs auxquels vous souhaitez donner accès à l'application AWS Supply Chain Web. Choisissez Invite Users. Pour plus d'informations sur la façon d'ajouter des utilisateurs à IAM Identity Center, consultezAjouter des utilisateurs dans IAM Identity Center. Pour plus d'informations sur les rôles AWS Supply Chain d'autorisation des utilisateurs, consultezRôles d'autorisation utilisateur.
4. Si vous souhaitez ajouter des utilisateurs ultérieurement, vous pouvez choisir Ignorer pour le moment.

La page complète de l'intégration apparaît.

5. Chaque utilisateur que vous avez ajouté reçoit un e-mail contenant un lien vers AWS Supply Chain, ou vous pouvez choisir Copier le lien et envoyer le lien aux utilisateurs.
6. Choisissez Continuer vers la page d'accueil pour afficher le AWS Supply Chain tableau de bord.

Mettre à jour le profil de votre compte

Vous pouvez mettre à jour le profil de votre compte à tout moment sur l'application AWS Supply Chain Web. Suivez ces étapes pour mettre à jour le compte.

1. Sur le tableau de bord de l'application AWS Supply Chain Web, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres.
2. Choisissez le profil du compte.

   La page Profil du compte apparaît.
3. Mettez à jour les informations du compte, puis choisissez Enregistrer.

Mettre à jour le profil de votre organisation

Vous pouvez mettre à jour le profil de l'organisation à tout moment sur l'application AWS Supply Chain Web. Suivez ces étapes pour mettre à jour le profil de l'organisation.

1. Sur le tableau de bord de l'application AWS Supply Chain Web, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres.
2. Choisissez Organisation, puis Profil de l'organisation.

   La page Profil de l'organisation apparaît.
3. Mettez à jour le logo de l'organisation ou l'emplacement du siège social, puis choisissez Enregistrer.

Rôles d'autorisation utilisateur

En tant qu' AWS Supply Chain administrateur, vous pouvez utiliser les rôles d'autorisation utilisateur par défaut ou créer des rôles d'autorisation personnalisés. AWS Supply Chain possède les rôles d'autorisation utilisateur par défaut suivants :

- Administrateur : accès permettant de créer, d'afficher et de gérer toutes les données et les autorisations des utilisateurs.
- Analyste de données : accès permettant de créer, d'afficher et de gérer toutes les connexions de données.
- Gestionnaire d'inventaire : accès permettant de créer, d'afficher et de gérer des informations.
- Planificateur : accès pour créer, consulter et gérer les prévisions, les dérogations et publier des plans de demande.
- Gestionnaire de données sur les partenaires : accès permettant de gérer et de consulter les partenaires, de gérer et de consulter les demandes de données et de consulter les données sur le développement durable.
- Planificateur d'approvisionnement — Accès pour gérer et consulter les plans d'approvisionnement.

> **Note**
>
> En tant qu' AWS Supply Chain administrateur, avant d'ajouter des utilisateurs, prenez note des points suivants :
>
> - Chaque rôle d'autorisation utilisateur par défaut est défini avec un ensemble d'autorisations. Vous pouvez ajouter des utilisateurs aux rôles d'autorisation utilisateur par défaut ou créer des rôles d'autorisation personnalisés.
> - Un utilisateur ne peut être affecté qu'à un seul rôle d'autorisation utilisateur.
> - Vous ne pouvez pas modifier ou supprimer les rôles d'autorisation utilisateur par défaut.
> - Lorsque vous modifiez un rôle d'autorisation personnalisé que vous avez créé, les autorisations de tous les utilisateurs du rôle d'autorisation personnalisé sont mises à jour.
> - Lorsque vous supprimez un rôle d'autorisation personnalisé que vous avez créé, tous les utilisateurs associés au rôle d'autorisation personnalisé n'y ont plus accès AWS Supply Chain.
> - L'ajout de groupes n'est pas pris en charge dans AWS Supply Chain.

Rubriques

Ajout d'utilisateurs

> **Note**
>
> Avant d'ajouter des utilisateurs, assurez-vous que l'utilisateur fait partie d'un groupe IAM Identity Center auquel le groupe est affecté. AWS Supply Chain

En tant qu' AWS Supply Chain administrateur, vous pouvez ajouter des utilisateurs pour accéder à l'application AWS Supply Chain Web. Pour ajouter un utilisateur, procédez comme suit.

1. Sur le AWS Supply Chain tableau de bord, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres.
2. Choisissez Autorisations, puis Utilisateurs.

   La page Gérer les utilisateurs s'affiche.
3. Choisissez Ajouter un nouvel utilisateur.

   La page Ajouter un utilisateur apparaît.
4. Dans le menu déroulant Ajouter un ou plusieurs utilisateurs, sélectionnez l'utilisateur, puis sous Sélectionner un rôle, sélectionnez le rôle de l'utilisateur.
5. Choisissez Ajouter.

Mettre à jour les autorisations des utilisateurs

Vous pouvez mettre à jour le rôle d'autorisation utilisateur pour les AWS Supply Chain utilisateurs actuels. Suivez ces étapes pour mettre à jour le rôle d'autorisations utilisateur.

1. Sur le AWS Supply Chain tableau de bord, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres.
2. Choisissez Autorisations, puis Utilisateurs.

   La page Gérer les utilisateurs s'affiche.
3. Sur la page Gérer les utilisateurs, sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez mettre à jour le rôle d'autorisation utilisateur, puis dans le menu déroulant Rôle d'autorisation, sélectionnez l'un des rôles d'autorisation ci-dessous :

> **Note**
>
> En fonction des autorisations de rôle que vous attribuez, le AWS Supply Chain tableau de bord est personnalisé. Pour plus d'informations, consultez Création de rôles d'autorisation utilisateur personnalisés.

- Administrateur : accès permettant de créer, d'afficher et de gérer toutes les données et les autorisations des utilisateurs.
- Analyste de données : accès permettant de créer, d'afficher et de gérer toutes les connexions de données.
- Gestionnaire d'inventaire : accès permettant de créer, d'afficher et de gérer des informations.
- Planificateur : accès pour créer, consulter et gérer les prévisions, les dérogations et publier des plans de demande.

4. Choisissez Enregistrer.

Suppression des utilisateurs

En tant AWS Supply Chain qu'administrateur, vous pouvez supprimer des utilisateurs de l'application AWS Supply Chain Web. Pour supprimer des utilisateurs, procédez comme suit.

1. Sur le AWS Supply Chain tableau de bord, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres.
2. Choisissez Autorisations, puis Utilisateurs.

   La page Gérer les utilisateurs s'affiche.
3. Sur la page Gérer les utilisateurs, sélectionnez l'utilisateur que vous souhaitez supprimer et cliquez sur l'icône Supprimer.

Création de rôles d'autorisation utilisateur personnalisés

Outre les rôles d'autorisation utilisateur par défaut, vous pouvez créer des rôles d'autorisation utilisateur personnalisés pour inclure plusieurs rôles d'autorisation et ajouter des emplacements et des produits spécifiques. Suivez ces étapes pour créer de nouveaux rôles d'autorisation.

> **Note**
>
> Vous ne pouvez choisir les produits et les emplacements sous Accès à la localisation et Accès au produit que si votre instance est connectée à une source de données. Par exemple, vous pouvez créer un utilisateur administrateur personnalisé uniquement pour gérer les avocats sur le site de Seattle, ou un utilisateur Insight uniquement pour gérer les informations relatives aux avocats sur le site de Seattle.

1. Sur le AWS Supply Chain tableau de bord, dans le volet de navigation de gauche, cliquez sur l'icône Paramètres. Choisissez Autorisations, puis sélectionnez Rôles d'autorisation.

   La page Rôles d'autorisation apparaît.
2. Choisissez Create New Role (Créer un nouveau rôle).
3. Sur la page Gérer le rôle d'autorisation, sous Nom du rôle, entrez un nom.
4. Déplacez le curseur pour sélectionner le rôle d'autorisation de l'utilisateur.

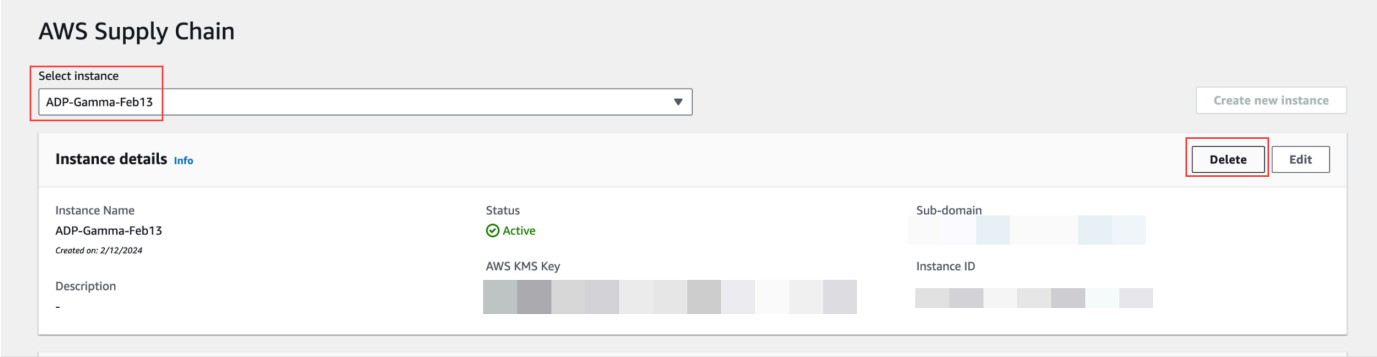
   - Gérer — L'attribution d'autorisations de gestion à des utilisateurs permet d'ajouter, de modifier et de gérer des informations.
   - Afficher — L'attribution aux utilisateurs d'une autorisation de consultation ne peut afficher que les informations actuelles.
5. Sous Accès à la localisation, recherchez les régions au fur et à mesure que vous tapez dans la barre de recherche et sélectionnez les régions.
6. Sous Accès aux produits, recherchez les produits au fur et à mesure que vous les tapez dans la barre de recherche et sélectionnez les produits.
7. Choisissez Enregistrer.

Suppression d'une instance

Pour supprimer une instance, procédez comme suit.

> **Note**
>
> Lorsque vous supprimez une instance, les informations du compartiment Amazon S3 ne sont pas automatiquement supprimées.

1. Ouvrez la AWS Supply Chain console à l'adressehttps://console.aws.amazon.com/scn/home.
2. Sur le tableau de bord de la AWS Supply Chain console, dans le menu déroulant, sélectionnez l'instance que vous souhaitez supprimer.



3. Sélectionnez Delete (Supprimer).
4. Sur la page Supprimer l' AWS Supply Chain instance, sous Confirmation, tapez **`delete`** pour confirmer que vous souhaitez supprimer l'instance.
5. Sélectionnez Delete (Supprimer). La suppression de l'instance commence et une fois l'instance supprimée, vous verrez un message de confirmation.

Sécurité dans AWS Supply Chain

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 AWS répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous et AWS. 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 s'exécute Services AWS 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 conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Supply Chain, voir AWS Services concernés par programme de conformité AWS .
- Sécurité dans le cloud — Service AWS Ce que vous utilisez détermine votre responsabilité. Vous êtes également responsable d'autres facteurs, notamment de la sensibilité de vos données, de vos exigences et des lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous l'utilisez AWS Supply Chain. Les rubriques suivantes expliquent comment procéder à la configuration AWS Supply Chain pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser vos AWS Supply Chain ressources.

Rubriques

Protection des données dans AWS Supply Chain

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Supply Chain. 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 en savoir plus 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.
- 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 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus 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 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 Name (Nom). Cela inclut lorsque vous travaillez avec AWS Supply Chain ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données

que vous saisissez 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.

Données traitées par AWS Supply Chain

Pour limiter les données accessibles aux utilisateurs autorisés d'une instance de chaîne d' AWS approvisionnement spécifique, les données détenues dans la chaîne AWS d'approvisionnement sont séparées par votre identifiant de AWS compte et votre identifiant d'instance de chaîne AWS d'approvisionnement.

AWS La chaîne d'approvisionnement gère diverses données de la chaîne d'approvisionnement, telles que les informations utilisateur, les informations extraites du connecteur de données et les détails de l'inventaire.

Préférence de désabonnement

Nous pouvons utiliser et stocker votre contenu traité par AWS Supply Chain, comme indiqué dans les conditions de service AWS. Si vous souhaitez refuser d'utiliser ou AWS Supply Chain de stocker votre contenu, vous pouvez créer une politique de désinscription dans AWS Organizations. Pour plus d'informations sur la création d'une politique de désinscription, consultez la syntaxe et les exemples de politique de désinscription des services d'intelligence artificielle.

Chiffrement au repos

Les données de contact classées comme des informations personnelles, ou des données représentant le contenu client stocké par AWS Supply Chain, sont chiffrées au repos (c'est-à-dire avant d'être placées, stockées ou enregistrées sur un disque) à l'aide d'une clé limitée dans le temps et spécifique à l' AWS Supply Chain instance.

Le chiffrement côté serveur Amazon S3 est utilisé pour chiffrer toutes les données de console et d'application Web à l'aide d'une clé de AWS Key Management Service données unique pour chaque compte client. Pour plus d'informations AWS KMS keys, voir Qu'est-ce que c'est AWS Key Management Service ? dans le Guide AWS Key Management Service du développeur.

> **Note**
>
> AWS Supply Chain fonctionnalités La planification des approvisionnements et la visibilité N-Tier ne prennent pas en charge le chiffrement data-at-rest avec le KMS-CMK fourni.

Chiffrement en transit

Les données échangées avec AWS Supply Chain sont protégées pendant le transit entre le navigateur Web de l'utilisateur et AWS Supply Chain à l'aide d'un cryptage TLS conforme aux normes du secteur.

Gestion des clés

AWS Supply Chain supporte partiellement KMS-CMK.

Pour plus d'informations sur la mise à jour de la clé AWS KMS dans AWS Supply Chain, consultezCréation d'une instance.

Confidentialité du trafic inter-réseaux

> **Note**
>
> AWS Supply Chain ne prend pas en charge PrivateLink.

Un point de terminaison de cloud privé virtuel (VPC) pour AWS Supply Chain est une entité logique au sein d'un VPC qui autorise la connectivité uniquement à. AWS Supply Chain Le VPC achemine les demandes AWS Supply Chain et les réponses vers le VPC. Pour plus d'informations, consultez la section Points de terminaison VPC dans le guide de l'utilisateur VPC.

Comment AWS Supply Chain utilise les subventions dans AWS KMS

AWS Supply Chain nécessite une autorisation pour utiliser votre clé gérée par le client.

AWS Supply Chain crée plusieurs autorisations à l'aide de la AWS KMS clé transmise lors de l'CreateInstanceopération. AWS Supply Chain crée une subvention en votre nom en envoyant des CreateGrantdemandes à AWS KMS. Les subventions AWS KMS sont utilisées pour donner AWS Supply Chain accès à la AWS KMS clé d'un compte client.

> **Note**
>
> AWS Supply Chain utilise son propre mécanisme d'autorisation. Une fois qu'un utilisateur est ajouté AWS Supply Chain, vous ne pouvez pas refuser de répertorier le même utilisateur en utilisant la AWS KMS politique.

AWS Supply Chain utilise la subvention pour ce qui suit :

- Pour envoyer GenerateDataKeydes demandes AWS KMS de chiffrement des données stockées dans votre instance.
- Pour envoyer des demandes de déchiffrement AWS KMS afin de lire les données chiffrées associées à l'instance.
- Pour ajouter DescribeKeyCreateGrant, et RetireGrantautorisations afin de protéger vos données lorsque vous les envoyez à d'autres AWS services tels qu'Amazon Forecast.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, vous AWS Supply Chain ne pourrez accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données.

Surveillance de votre chiffrement pour AWS Supply Chain

Les exemples suivants sont AWS CloudTrail des événements destinés à `EncryptGenerateDataKey`, et `Decrypt` pour surveiller les opérations KMS appelées AWS Supply Chain pour accéder aux données chiffrées par votre clé gérée par le client :

Encrypt


```
          {
"eventVersion": "1.08",
"userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
},
"eventTime": "2024-03-06T22:39:32Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Encrypt",
"awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
```

```
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
```

```
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Accès AWS Supply Chain via un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et. AWS Supply Chain Vous pouvez y accéder AWS Supply Chain comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour y accéder. AWS Supply Chain

Vous établissez cette connexion privée en créant un point de terminaison d’interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d’interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à AWS Supply Chain.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Considérations relatives à AWS Supply Chain

Avant de configurer un point de terminaison d'interface pour AWS Supply Chain, consultez les considérations du AWS PrivateLink guide.

AWS Supply Chain prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Créez un point de terminaison d'interface pour AWS Supply Chain

Vous pouvez créer un point de terminaison d'interface pour AWS Supply Chain utiliser la console Amazon VPC ou le AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour AWS Supply Chain utiliser le nom de service suivant :

```
com.amazonaws.region.scn
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à AWS Supply Chain l'aide de son nom DNS régional par défaut. Par exemple, *scn*.*region*.amazonaws.com.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet AWS Supply Chain via le point de terminaison de l'interface. Pour contrôler l'accès autorisé AWS Supply Chain depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWSutilisateurs IAM et rôles IAM)
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être effectuées

Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions AWS Supply Chain

Voici un exemple de politique de point de terminaison. Lorsque vous attachez cette politique à votre point de terminaison d'interface, elle accorde l'accès aux actions AWS Supply Chain répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

         ],
         "Resource":"*"
      }
   ]
}
```

IAM pour AWS Supply Chain

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 IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS Supply Chain les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment AWS Supply Chain fonctionne avec IAM

- Exemples de politiques basées sur l’identité pour AWS Supply Chain
- Résolution des problèmes AWS Supply Chain d'identité et d'accès

Public ciblé

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

Utilisateur du service : si vous utilisez le AWS Supply Chain service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS Supply Chain fonctionnalités 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 pouvez pas accéder à une fonctionnalité dans AWS Supply Chain, consultez Résolution des problèmes AWS Supply Chain d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS Supply Chain ressources de votre entreprise, vous avez probablement un accès complet à AWS Supply Chain. C'est à vous de déterminer les AWS Supply Chain fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM 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 AWS Supply Chain, voirComment AWS Supply Chain fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d’écrire des politiques pour gérer l’accès à AWS Supply Chain. Pour consulter des exemples de politiques AWS Supply Chain basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l’identité pour AWS Supply Chain

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs

(IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être 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 Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface 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. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 Quand créer un utilisateur IAM (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. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM 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 Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

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

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'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. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant 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 instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez 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 à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. 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 Vue d'ensemble 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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez 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 découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne 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. Des politiques basées sur les ressources sont, par exemple, les politiques de

confiance de rôle IAM et des politiques de compartiment. 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 dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier 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 (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes 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.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS 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 les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- 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 séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. 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 politiques de séance 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 AWS Supply Chain fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Supply Chain, découvrez les fonctionnalités IAM disponibles. AWS Supply Chain

Fonctionnalités IAM que vous pouvez utiliser avec AWS Supply Chain

Fonction IAM	AWS Supply Chain soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non

Fonction IAM	AWS Supply Chain soutien
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d’une politique	Oui
Informations d’identification temporaires	Oui
Transmission des sessions d’accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AWS Supply Chain les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS Supply Chain

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et 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 une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Exemples de politiques basées sur l'identité pour AWS Supply Chain

Pour consulter des exemples de politiques AWS Supply Chain basées sur l'identité, consultez. Exemples de politiques basées sur l’identité pour AWS Supply Chain

Politiques basées sur les ressources au sein de AWS Supply Chain

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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 dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier 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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L’ajout d’un principal entre comptes à une politique basée sur les ressources ne représente qu’une partie de l’instauration de la relation d’approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l’entité. Toutefois, si une politique basée sur des ressources accorde l’accès à un principal dans le même compte, aucune autre politique basée sur l’identité n’est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour AWS Supply Chain

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 quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

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

Les actions de politique en AWS Supply Chain cours utilisent le préfixe suivant avant l'action :

```
scn
```

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

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

Pour consulter des exemples de politiques AWS Supply Chain basées sur l'identité, consultez. [Exemples de politiques basées sur l'identité pour AWS Supply Chain]

Ressources politiques pour AWS Supply Chain

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 sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter des exemples de politiques AWS Supply Chain basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Supply Chain

Clés de conditions de politique pour AWS Supply Chain

Prend en charge les clés de condition de politique spécifiques au service	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 `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` 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 `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource

uniquement si elle est balisée avec son nom d'utilisateur IAM. 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 voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter des exemples de politiques AWS Supply Chain basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Supply Chain

Utilisation d'informations d'identification temporaires avec AWS Supply Chain

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 Changement de 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.

Transférer les sessions d'accès pour AWS Supply Chain

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS Supply Chain

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. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'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 AWS Supply Chain les fonctionnalités. Modifiez les rôles de service uniquement lorsque AWS Supply Chain vous recevez des instructions à cet effet.

Rôles liés à un service pour AWS Supply Chain

Prend en charge les rôles liés à un service	Non

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 au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM 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 AWS Supply Chain

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier AWS Supply Chain des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 IAM dans le guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS Supply Chain des ressources 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 AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d’informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l’utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l’exécution d’une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des

ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Résolution des problèmes AWS Supply Chain d'identité et d'accès

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

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Supply Chain
- Je ne suis pas autorisé à effectuer iam : PassRole

- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Supply Chain ressources

Je ne suis pas autorisé à effectuer une action dans AWS Supply Chain

Si vous AWS Management Console n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

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 `scn:`*`GetWidget`* fictives.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `scn:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Supply Chain.

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, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS Supply Chain. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

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

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Supply Chain ressources

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 (ACL), vous pouvez utiliser ces politiques pour donner l’accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Supply Chain en charge, consultezComment AWS Supply Chain 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 par le biais de la fédération d’identité, consultez Fournir un accès à des utilisateurs authentifiés en 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 Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Politiques AWS gérées pour AWS Supply Chain

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d’utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l’esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d’utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d’utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu’un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d’informations, consultez la section Politiques gérées par AWS dans le Guide de l’utilisateur IAM.

AWSpolitique gérée : AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess fournit aux utilisateurs AWS Supply Chain fédérés l'accès à l'AWS Supply Chainapplication, y compris les autorisations requises pour effectuer des actions au sein de l'AWS Supply Chainapplication. La politique fournit des autorisations administratives aux utilisateurs et aux groupes IAM Identity Center et est attachée à un rôle créé par AWS Supply Chain vous. Vous ne devez associer la AWSSupplyChainFederationAdminAccess politique à aucune autre entité IAM.

Bien que cette politique fournisse tous les accès AWS Supply Chain via les autorisations scn : *, le AWS Supply Chain rôle détermine vos autorisations. Le AWS Supply Chain rôle inclut uniquement les autorisations requises et ne dispose pas d'autorisations pour accéder aux API d'administration.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes :

- `Chime`— Permet de créer ou de supprimer des utilisateurs sous un Amazon Chime AppInstance ; fournit un accès pour gérer la chaîne, les membres de la chaîne et les modérateurs ; fournit un accès pour envoyer des messages à la chaîne. Les opérations Chime sont limitées aux instances d'application étiquetées « InstanceId SCN ».

- `AWS IAM Identity Center (AWS SSO)`— Fournit les autorisations requises pour associer et dissocier les profils utilisateur et répertorier les profils associés à l'instance d'application IAM Identity Center.
- `AppFlow`— Fournit un accès pour créer, mettre à jour et supprimer des profils de connexion ; fournit un accès pour créer, mettre à jour, supprimer, démarrer et arrêter des flux ; fournit un accès pour étiqueter et débaliser les flux et décrire les enregistrements de flux.
- `Amazon S3`— Permet d'accéder à la liste de tous les compartiments. Fournit GetBucketLocation, GetBucketPolicy, PutObject GetObject, et un ListBucket accès aux buckets avec un arn de ressources arn:aws:s3 : a:-*. aws-supply-chain-data
- `SecretsManager`— Permet de créer des secrets et de mettre à jour la politique secrète.
- `KMS`— Fournit au AppFlow service Amazon l'accès aux clés de liste et aux alias de clés. Fournit DescribeKey CreateGrant et autorise ListGrants les clés KMS étiquetées avec la valeur clé aws-suply-chain-access : true ; fournit un accès pour créer des secrets et mettre à jour la politique secrète.

  Les autorisations (kms : ListKeys, kms : ListAliases, kms : GenerateDataKey et KMS:Decrypt) ne sont pas limitées à Amazon AppFlow et peuvent être accordées à n'importe quelle AWS KMS clé de votre compte.

Pour consulter les autorisations associées à cette politique, consultez AWSSupplyChainFederationAdminAccessleAWS Management Console.

Mises à jour AWS Supply Chain vers des politiques gérées par AWS

Le tableau suivant répertorie les informations relatives aux mises à jour apportées aux politiques AWS gérées AWS Supply Chain depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document AWS Supply Chain.

Modification	Description	Date
AWSSupplyChainFederationAdminAccess— Politique mise à jour	AWS Supply Chaina mis à jour la politique gérée pour permettre aux utilisateurs	01 novembre 2023

Modification	Description	Date
	fédérés d'accéder aux ListProfi leAssociations opérations dans IAM Identity Center.	
AWSSupplyChainFede rationAdminAccess— Politique mise à jour	AWS Supply Chaina mis à jour la politique gérée pour permettre aux utilisate urs fédérés d'accéder aux GetObject opérations PutObject et sur le compartim ent S3 dédié avec la ressource arn arn:aws:s 3 : ::aws-supply- chain-data-*.	21 septembre 2023
AWSSupplyChainFede rationAdminAccess – Nouvelle politique	AWS Supply Chaina ajouté une nouvelle politique permettant aux utilisateurs fédérés d'accéder à l'AWS Supply Chainapplication. Cela inclut les autorisations nécessaires pour effectuer des actions au sein de l'AWS Supply Chainapplication.	01 mars 2023
AWS Supply Chain a démarré le suivi des modifications	AWS Supply Chain a commencé à suivre les modifications pour ses politiques gérées par AWS.	01 mars 2023

Validation de la conformité pour AWS Supply Chain

Les auditeurs tiers évaluent la sécurité et la conformité de AWS Supply Chain dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et autres.

Pour obtenir une liste des services relevant deServices AWS programmes spécifiques, veuillez consulter AWSServices relevant de programmes relevant de programmes relevant de programmes relevant de programmes relevant de programmes relevant de programmes relevant de programmes relevant de programmes relevant de programmesAWS relevant de programmes relevant Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger des rapports d'audit externe avecAWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de votre utilisationAWS Supply Chain est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWSfournit les ressources suivantes pour faciliter la conformité :

- Guides Quick Start de de la sécurité et de la conformité : ces guides de déploiement proposent des considérations architecturales et fournissent des étapes pour déployer desAWS environnements de référence centrés sur la sécurité et la conformité sur.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à HIPAA.
- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide duAWS Config développeur : ce guide évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub— CelaService AWS fournit une vue complète de votre état de sécuritéAWS au sein d', ce qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques.

Résilience dans AWS Supply Chain

L'infrastructureAWS mondiale d'repose surRégions AWS des zones de disponibilité. Régions AWSfournir plusieurs zones de disponibilité physiquement séparées et isolées. Rattachées avec un réseau à latence faible, à débit élevé et à forte redondance Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l’échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Outre l'infrastructure globale AWS, AWS Supply Chain propose plusieurs fonctionnalités qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

Journalisation et surveillance AWS Supply Chain

La journalisation et la surveillance jouent un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de la chaîne AWS d'approvisionnement et de vos autres AWS solutions. AWS fournit l'outil AWS CloudTrail de surveillance permettant de surveiller la chaîne AWS d'approvisionnement, de signaler les problèmes et de prendre des mesures automatiques le cas échéant.

> **Note**
>
> Les API appelées uniquement depuis la AWS Supply Chain console sont capturées dans AWS CloudTrail.

AWS CloudTrail capture les appels d'API et les événements associés créés par votre Compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Vous pouvez consulter les événements de la chaîne AWS d'approvisionnement sur scn.amazonaws.com. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

> **Note**
>
> Notez ce qui suit avec AWS Supply Chain :
>
> - Lorsque vous invitez des utilisateurs qui n'y ont pas accès AWS Supply Chain, ces utilisateurs ne reçoivent aucune information dans les notifications qu'ils reçoivent de l'application Web. Les utilisateurs invités reçoivent une notification par e-mail contenant un lien vers l'application Web. Ils ne peuvent se connecter et consulter le contenu de la notification que s'ils disposent des autorisations utilisateur requises.

- Tous les utilisateurs autorisés ou non à accéder à un Insight en particulier peuvent consulter les messages du chat Insights.
- En tant qu'administrateur de l'application, lorsque vous ajoutez des utilisateurs à l' AWS Supply Chain instance, ils ont accès au AWS KMS key. Vous pouvez gérer les autorisations des utilisateurs pour ajouter ou supprimer des utilisateurs. Pour plus d'informations sur les autorisations des utilisateurs, consultezRôles d'autorisation utilisateur.

AWS Supply Chain événements de données dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture de données dans un objet Amazon S3). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de AWS Supply Chain ressources à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API.

- Pour enregistrer les événements de données à l'aide de la CloudTrail console, créez un magasin de données de suivi ou d'événement pour enregistrer les événements, ou mettez à jour un magasin de données de suivi ou d'événement existant pour enregistrer les événements de données.

  1. Choisissez Data events pour enregistrer les événements liés aux données.
  2. Dans la liste des types d'événements de données, choisissez le type de ressource pour lequel vous souhaitez enregistrer les événements de données.
  3. Choisissez le modèle de sélecteur de journal que vous souhaitez utiliser. Vous pouvez enregistrer tous les événements de données pour le type de ressource, consigner tous les `readOnly` événements, consigner tous les `writeOnly` événements ou créer un modèle de sélecteur de journal personnalisé pour filtrer les `resources.`ARN champs `readOnly`et `eventName`, et.

- Pour enregistrer des événements de données à l'aide de AWS CLI, configurez le `--advanced-event-selectors` paramètre pour définir le `eventCategory` champ égal à la valeur du type de ressource `Data` et le `resources.type` champ égal à la valeur du type de ressource. Vous pouvez ajouter des conditions pour filtrer les valeurs des `resources.ARN` champs `readOnly`eventName, et.
  - Pour configurer un suivi afin de consigner les événements liés aux données, exécutez la put-event-selectorscommande. Pour plus d'informations, consultez la section Enregistrement des événements de données pour les sentiers avec le AWS CLI.
  - Pour configurer un magasin de données d'événements afin de consigner les événements, exécutez la create-event-data-storecommande pour créer un nouveau magasin de données d'événements pour enregistrer les événements ou exécutez la update-event-data-storecommande pour mettre à jour un magasin de données d'événements existant. Pour plus d'informations, consultez la section Enregistrement des événements de données pour les magasins de données d'événements avec le AWS CLI.

*Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les `eventName`readOnly, et des `resources.ARN` champs pour enregistrer uniquement les événements qui sont importants pour vous. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelector.

AWS Supply Chain événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS Supply Chain enregistre toutes les opérations du plan de contrôle CloudTrail sous forme d'événements de gestion.

AWS Supply Chain API d'applications Web

Les API répertoriées dans cette section sont appelées par AWS Supply Chain des applications pour le compte d'utilisateurs fédérés. Ces API ne sont pas visibles dans les CloudTrail journaux et ne sont pas capturées dans le document de référence d'autorisation de service, voir AWS Supply Chain. L'accès à ces API est contrôlé par les AWS Supply Chain applications en fonction des autorisations de rôle d'utilisateur fédérées. Vous ne devez pas essayer de contrôler l'accès à ces API pour éviter de perturber les AWS Supply Chain applications.

Rôles utilisateurs

Les API suivantes sont utilisées pour gérer les utilisateurs, les rôles des utilisateurs, les notifications utilisateur et les messages de chat dans AWS Supply Chain.

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
```

```
scn:UpdateRole
scn:UpdateUser
```

Lac de données

Les API suivantes sont utilisées pour créer et gérer les flux de données et les connexions dans le lac de données.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Informations

Les API suivantes sont utilisées par l'application Insights pour gérer les filtres, les listes de suivi et afficher les modifications d'inventaire.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
```

```
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Planification de la demande

Les API suivantes sont utilisées pour AWS Supply Chain créer et gérer des prévisions, des plans de demande ou des classeurs.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
```

```
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Planification des approvisionnements

Les API suivantes sont utilisées pour AWS Supply Chain créer et gérer des plans d'approvisionnement.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
```

```
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Quotas pour AWS Supply Chain

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander une augmentation des quotas pour les ressources définies au niveau de votre compte. Pour plus d'informations sur les quotas au niveau des comptes, consultez le tableau ci-dessous.

Pour consulter les quotas pour AWS Supply Chain, ouvrez la console Service Quotas. Dans le panneau de navigation, sélectionnez Services AWS , puis AWS Supply Chain.

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le formulaire d'augmentation des limites.

Vous Compte AWS disposez des quotas suivants relatifs à AWS Supply Chain.

Ressource	Par défaut	Ajustable
Nombre d'instances **Note** Vous pouvez créer jusqu'à 10 instances dans un AWS compte.	10	Non
Nombre de compartiments Amazon S3	100	Non
Invitations actives et en attente au sein d'un AWS compte	30	Oui
Demandes de données au sein d'un AWS compte	4 000	Oui

Ressource	Par défaut	Ajustable
Eléments de la rubrique Insights par liste de suivi	1 000	Non
Listes de surveillance Insights par instance au sein d'un compte AWS	1 000	Oui
Listes de suivi Insights par utilisateur au sein d'un compte AWS	100	Oui

Support administratif pour AWS Supply Chain

Si vous êtes administrateur et que vous avez besoin de contacter le service de support pour AWS Supply Chain, choisissez l'une des options suivantes :

- Si vous avez unAWS Support compte, rendez-vous sur le Centre d'Support et soumettez un ticket.
- Ouvrez le dossier AWS Management Consoleet choisissez AWSSupply Chain, Support, Create.

Il est utile de fournir les informations suivantes :

- L'ID/ARN de votre instance de chaîne d'AWSapprovisionnement.
- VotreAWS région.
- Description détaillée de votre problème.

Historique du document pour le guide de AWS Supply Chain l'administrateur

Le tableau suivant décrit les versions de documentation pour AWS Supply Chain.

Modification	Description	Date
Mise à jour des politiques KMS	Mise à jour de la politique KMS AWS Supply Chain pour autoriser l'accès à votre AWS KMS clé.	18 mars 2024
PrivateLink soutien	Vous pouvez y accéder à AWS Supply Chain l'aide d'un point de terminaison d'interface (AWS PrivateLink).	26 février 2024
Ajouter des groupes	Les utilisateurs doivent faire partie d'un groupe IAM Identity Center pour y accéder AWS Supply Chain.	14 novembre 2023
Politique AWS gérée mise à jour	AWS Supply Chain a mis à jour la politique gérée pour permettre aux utilisateurs fédérés d'accéder aux ListProfileAssociations opérations dans IAM Identity Center.	1er novembre 2023
Politique AWS gérée mise à jour	AWS Supply Chain a mis à jour la politique gérée pour permettre aux utilisateurs fédérés d'accéder au bucket Amazon S3 dédié PutObject et aux GetObject opérations sur celui-ci avec la ressource	21 septembre 2023

	arn arn:aws:s3 : ::aws-supply-chain-data-*.	
Informations mises à jour sur le soutien aux régions	AWS Supply Chain La planification de la demande est désormais également prise en charge dans la région Asie-Pacifique (Sydney).	12 septembre 2023
Utiliser AWS la console pour s'inscrire et se désinscrire AWS Supply Chain	AWS Supply Chain les utilisateurs peuvent désormais utiliser la AWS console pour s'inscrire ou refuser AWS Supply Chain d'utiliser ou de stocker votre contenu sur AWS Organizations.	7 septembre 2023
Informations mises à jour sur le soutien aux régions	AWS Supply Chain est désormais également pris en charge dans la région Asie-Pacifique (Sydney) et dans la région Europe (Irlande).	19 juillet 2023
Informations mises à jour sur la manière de contacter le support AWS et de créer une instance	AWS Supply Chain les utilisateurs peuvent désormais contacter AWS Support pour obtenir de l'aide et mettre à jour le contenu expliquant comment créer une instance.	3 avril 2023

Ajout d'une politique AWS gérée	AWS Supply Chain a ajouté une nouvelle politique permettant aux utilisateurs fédérés d'accéder à l'application AWS Supply Chain, y compris les autorisations nécessaires pour effectuer des actions dans l'application AWS Supply Chain.	1er mars 2023
Première version	Première publication du guide de AWS Supply Chain l'administrateur.	29 novembre 2022

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.