Guide de l'acheteur

AWS Marketplace

AWS Marketplace: Guide de l'acheteur

Table of Contents

Qu'est-ce que AWS Marketplace ?

AWS Marketplaceest un catalogue numérique organisé que vous pouvez utiliser pour trouver, acheter, déployer et gérer les logiciels, données et services tiers dont vous avez besoin pour créer des solutions et gérer votre entreprise.AWS Marketplaceinclut des milliers de listes de logiciels appartenant à des catégories populaires telles que la sécurité, les réseaux, le stockage, l'apprentissage automatique, l'IoT, l'informatique décisionnelle, les bases de données etDevOps.AWS Marketplacesimplifie également les licences et les achats de logiciels grâce à des options de tarification flexibles et à de multiples méthodes de déploiement. En outre,AWS Marketplaceinclut des produits de données disponibles auprès d'AWS Data Exchange.

Vous pouvez démarrer rapidement des logiciels préconfigurés en quelques clics et choisir des solutions logicielles aux formats Amazon Machine Image (AMI) et logiciel en tant que service (SaaS, Software as a Service), ainsi que d'autres. En outre, vous pouvez naviguer et vous abonner à des produits de données. Les options de tarification flexibles incluent un essai gratuit, une utilisation à l'heure, au mois, à l'année, sur plusieurs années et un modèle Bring Your Own License (BYOL). Toutes ces options de tarification sont facturées via une source unique. AWS gère la facturation et les paiements, les frais apparaissant sur votre facture AWS.

Vous pouvez utiliser AWS Marketplace en tant qu'acheteur (abonné) ou en tant que vendeur (fournisseur), ou les deux. Toute personne possédant unCompte AWSpeut utiliserAWS Marketplaceen tant que consommateur et peut s'inscrire pour devenir vendeur. Un vendeur peut être un fournisseur indépendant de logiciels (FIL), un revendeur à valeur ajoutée ou une personne qui a quelque chose à proposer qui fonctionne avec les produits et services AWS.

> **Note**
>
> Les fournisseurs de produits de données doivent satisfaire aux critères d'éligibilité d'AWS Data Exchange. Pour plus d'informations, voirFourniture de produits de données sur AWS Data Exchangedans leGuide de l'utilisateur d'AWS Data Exchange.

Chaque produit logiciel dans AWS Marketplace a été soumis à un processus de maintenance. La page du produit peut contenir une ou plusieurs offres pour le produit. Lorsque le vendeur envoie un produit dans AWS Marketplace, il définit le prix du produit et les conditions générales d'utilisation. Les acheteurs acceptent le prix, ainsi que les conditions générales définies pour l'offre.

DansAWS Marketplace, le produit peut être utilisé gratuitement ou peut être associé à des frais. Les frais sont inclus dans votre facture AWS et, une fois que vous avez payé, AWS Marketplace règle le vendeur.

> **Note**
>
> Lorsque vous achetez auprès de vendeurs non américains, vous pouvez également recevoir une facture fiscale de la part du vendeur. Pour de plus amples informations, veuillez consulter Vendeurs du Marketplace dans Aide sur les taxes Amazon Web Services.

Les produits peuvent prendre de nombreuses formes. Par exemple, un produit peut être proposé sous la forme d'une Amazon Machine Image (AMI) instanciée à l'aide de votreCompte AWS. Le produit peut également être configuré pour utiliser les modèles AWS CloudFormation pour la livraison au consommateur. Il peut aussi s'agir d'un SaaS (logiciel en tant que service) publié par un FIL, une ACL web, un ensemble de règles ou des conditions pour AWS WAF.

Vous pouvez acheter des produits logiciels au prix indiqué dans le contrat de licence de l'utilisateur final (CLUF) de l'éditeur ou proposés avec la tarification consommateur et le CLUF. Vous pouvez également acheter des produits dans le cadre d'uncontrat standardavec des limites de temps ou d'utilisation spécifiées.

Une fois que les abonnements aux produits sont en place, vous pouvez utiliserAWS Service Catalogpour copier le produit et gérer la manière dont le produit est accessible et utilisé dans votre organisation. Pour plus d'informations, voirAjouterAWS MarketplaceDes produits pour votre portefeuilledans leAWS Service CatalogGuide de l'administrateur.

Structure du contrat dansAWS Marketplace

Utilisation des logiciels, services et produits de données vendus surAWS Marketplaceest régi par des accords entre acheteurs et vendeurs.AWSn'est pas partie à ces accords.

En tant qu'acheteur, votre utilisation deAWS Marketplaceest régi par leConditions du service AWS, leContrat client AWS, et leAvis de confidentialité.

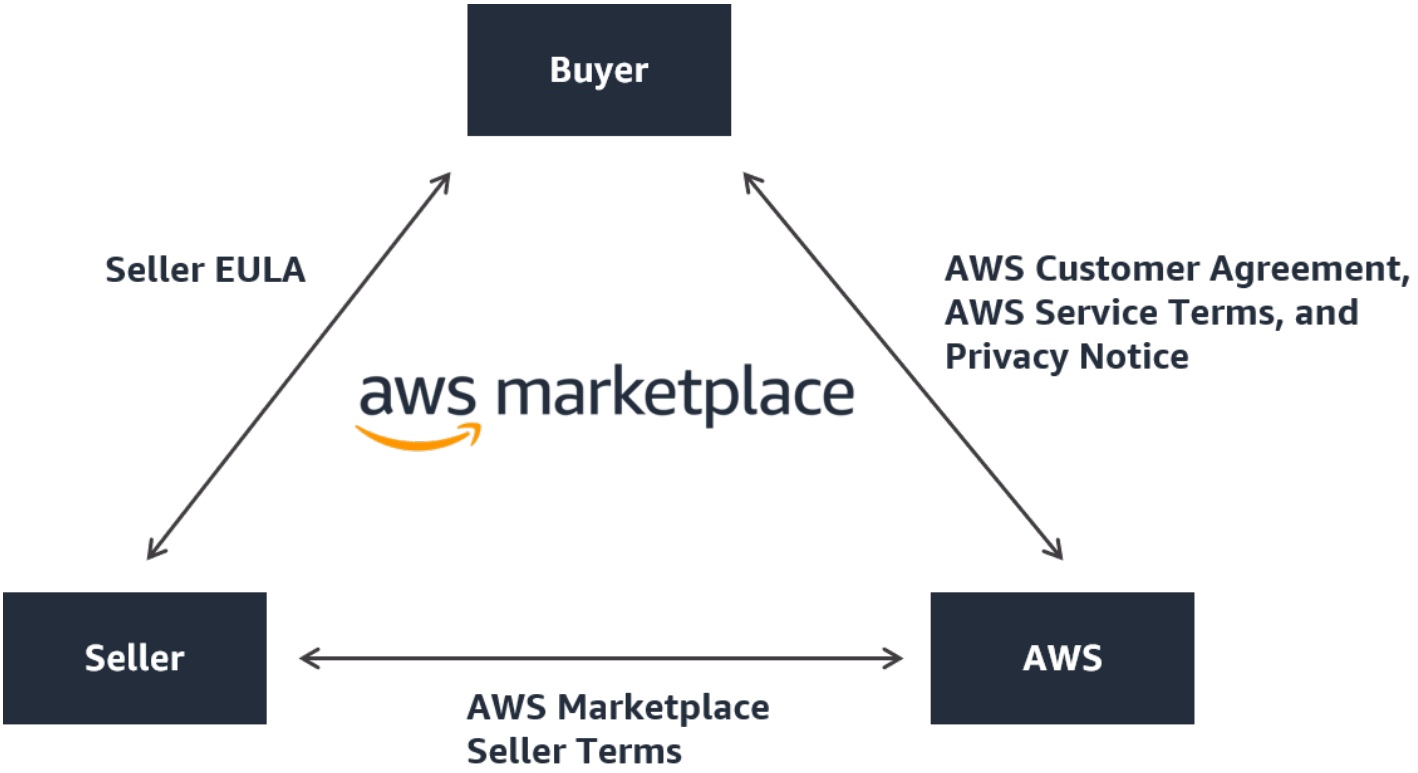
Les contrats de vente incluent les suivants :

- Le CLUF du vendeur se trouve sur la page de liste des produits pour les offres de logiciels publiques surAWS Marketplace. De nombreux vendeurs utilisent leContrat standard

pourAWS Marketplace(SCMP)comme leur EULA par défaut. Ils peuvent également utiliser le SCMP comme base de négociation dans le cadre d'offres privées et utiliser le modèle d'amendement pour modifier le SCMP. Les offres privées peuvent également inclure des conditions contractuelles personnalisées négociées entre les parties.

- AWS MarketplaceTermes du vendeurrégir l'activité du vendeur dansAWS Marketplace.

Le graphique suivant montre la structure du contrat pourAWS Marketplace.



Mises à jour du CLUF

Les vendeurs ont la possibilité de mettre à jour le CLUF pour chacun de leurs produits SaaS (Software as a Service). La date à laquelle cette mise à jour affecte votre EULA dépend du type d'offre et du modèle de tarification.

Le tableau suivant fournit des informations sur la date d'entrée en vigueur du nouvel EULA pour les produits SaaS.

Type d'offre	Modèle de tarification	Lorsque le CLUF mis à jour entre en vigueur
Public	Utilisation	Vous annulez votre abonnement et vous vous réabonnez.
Public	Contrat	Votre contrat actuel prend fin et se renouvelle pour devenir un nouveau contrat d'offre publique.
Public	Contrat avec consommation	Votre contrat actuel prend fin et se renouvelle pour devenir un nouveau contrat d'offre publique.
Privé	Utilisation	Votre offre privée actuelle expire et se renouvelle automatiquement dans le cadre d'un nouveau contrat d'offre publique. Les renouvell ements de l'offre privée dépendent de l'offre privée spécifique.
Privé	Contrat	Votre offre privée actuelle expire et vous vous réinscriv ez à l'offre publique ou à une nouvelle offre privée. Les renouvellements de l'offre privée dépendent de l'offre privée spécifique.
Privé	Contrat avec consommation	Votre offre privée actuelle expire et vous vous réinscriv ez à l'offre publique ou à une nouvelle offre privée. Les

Type d'offre	Modèle de tarification	Lorsque le CLUF mis à jour entre en vigueur
		renouvellements de l'offre privée dépendent de l'offre privée spécifique.

Contrats types pourAWS Marketplace

Lorsque vous vous préparez à acheter un produit, consultez le CLUF ou le contrat standardisé associé. De nombreux vendeurs proposent le même contrat standardisé sur leurs annonces, leContrat standard pourAWS Marketplace(SCMP).AWS Marketplacea développé le SCMP en collaboration avec les communautés d'acheteurs et de vendeurs afin de régir l'utilisation et de définir les obligations des acheteurs et des vendeurs pour les solutions numériques. Les exemples de solutions numériques incluent les logiciels de serveur, les logiciels en tant que service (SaaS) et les algorithmes d'intelligence artificielle et d'apprentissage automatique (AI/ML).

Au lieu de passer en revue les contrats de licence de l'utilisateur final (CLUF) personnalisés pour chaque achat, vous n'avez besoin de consulter le SCMP qu'une seule fois. Letermes du contratsont les mêmes pour tous les produits qui utilisent le SCMP.

Les vendeurs peuvent également utiliser les addenda suivants avec le SCMP :

- Addendum de sécurité amélioré— Prend en charge les transactions soumises à des exigences élevées en matière de sécurité des données.
- Addenda HIPAA Business Associate— Prend en charge les transactions conformément aux exigences de conformité à la loi de 1996 sur la portabilité et la responsabilité de l'assurance maladie (HIPAA).

Pour trouver des listes de produits proposant des contrats standardisés, utilisez leContrat standardfiltrer lors de la recherche de produits. Pour les offres privées, demandez au vendeur s'il peut remplacer son EULA par le SCMP et appliquer les modifications convenues si nécessaire pour répondre aux exigences spécifiques à la transaction.

Pour plus d'informations, voirContrats standardisés dansAWS Marketplace.

Utilisation d'AWS Marketplace comme acheteur

En tant qu'acheteur, vous allez àAWS Marketplacepour rechercher, filtrer et accéder à un produit qui fonctionne sur Amazon Web Services.

Lorsque vous choisissez un produit, vous êtes redirigé vers la page du produit. Celle-ci contient des informations sur le produit, la tarification, l'utilisation, l'assistance et les commentaires sur le produit. Pour vous abonner au produit logiciel, vous devez vous connecter à votreCompte AWSet sont redirigés vers une page d'abonnement contenant le CLUF, les conditions générales d'utilisation et toutes les options disponibles pour personnaliser votre abonnement.

AWS Marketplaceles achats effectués par le biais de vos comptes basés en Europe, au Moyen-Orient et en Afrique (à l'exception de la Turquie et de l'Afrique du Sud) auprès de vendeurs éligibles à la zone EMEA sont facilités par Amazon Web Services EMEA SARL.

Pour les clients de certains pays, Amazon Web Services EMEA SARL facture une taxe sur la valeur ajoutée (TVA) locale sur votreAWS Marketplaceachats. Pour plus d'informations sur les taxes, consultez lePage d'aide fiscale pour les acheteurs d'AWS Marketplace.

Pour plus d'informations sur Amazon Web Services EMEA SARL, consultez leFAQ sur Amazon Web Services EMEA SARL.

Les clients qui effectuent des transactions avec des vendeurs éligibles à la zone EMEA reçoivent une facture d'Amazon Web Services EMEA SARL. Toutes les autres transactions continuent d'être effectuéesAWSInc. Pour plus d'informations, voirPayer pour des produits.

Une fois l'abonnement traité, vous pouvez configurer les options d'expédition, les versions du logiciel etRégions AWSoù vous souhaitez utiliser le produit, puis lancez le produit logiciel. Vous pouvez également trouver ou lancer vos produits en vous rendant surVotre logiciel Marketplacesur leAWS Marketplacesite Web, depuis votreAWS Marketplaceou via la console Amazon Elastic Compute Cloud (Amazon EC2), ou via le catalogue de services.

Pour plus d'informations sur les catégories de produits disponibles à l'aide deAWS Marketplace, voirCatégories de produits.

Pour plus d'informations sur les méthodes de livraison des produits logiciels dansAWS Marketplace, voir :

- Produits pour serveurs basés sur l'AMI
- Produits de conteneur

- Produits de Machine Learning
- Produits de services professionnels
- Produits SaaS
- Produits de données — VoirQu'est-ce qu'AWS Data Exchange ?dans leGuide de l'utilisateur d'AWS Data Exchange

Logiciels et services sur AWS Marketplace

AWS Marketplacepropose plusieurs catégories de logiciels, notamment des bases de données, des serveurs d'applications, des outils de test, des outils de surveillance, gestion de contenu et Business Intelligence. Vous pouvez sélectionner des logiciels commerciaux publiés par des vendeurs connus, ainsi que de nombreux autres en open source qui sont largement utilisés. Lorsque vous trouvez un produit qui vous intéresse, vous pouvez acheter et déployer ce logiciel sur votre propre instance Amazon EC2 avec lancement en un clic. Vous pouvez également utiliserAWS CloudFormationpour déployer une topologie du produit.

AnyAWSle client peut faire ses achats surAWS Marketplace. Les prix des logiciels et les prix estimés de l'infrastructure sont affichés sur le site Web. Vous pouvez acheter la plupart des logiciels immédiatement, à l'aide de moyens de paiement déjà enregistrés auprès deAWS. Les frais du logiciel apparaissent sur la même facture mensuelle que les frais d'infrastructure AWS.

Remarques

- De nombreux produits professionnels sont disponibles dans leAWS Marketplace, notamment des produits SaaS (Software as a Service) et des produits basés sur des serveurs. Les produits basés sur des serveurs peuvent demander des connaissances techniques ou une assistance informatique pour leur configuration et leur maintenance.
- Les informations et les didacticiels deDidacticiel : Démarrez avec les instances Linux Amazon EC2peut vous aider à découvrir les bases d'Amazon EC2.
- Si vous envisagez de lancer des topologies complexes deAWS Marketplaceproduits viaAWS CloudFormation,Démarrer avec AWS CloudFormationpeut vous aider à découvrir AWS utile CloudFormation Bases.

AWS Marketplaceinclut les catégories suivantes de logiciels :

- Logiciels d'infrastructure
- Outils pour développeurs
- Logiciels métier
- Machine learning
- IoT
- Services professionnels
- Applications de bureau
- Produits de données

Pour plus d'informations, consultez Catégories de produits.

Chaque catégorie majeure de logiciels contient des sous-catégories plus spécifiques. Par exemple, la catégorie Logiciels d'infrastructure contient notamment les sous-catégories Développement d'applications, Bases de données et mise en cache et Systèmes d'exploitation. Les logiciels sont disponibles sous deux formes différentes, notamment Amazon Machine Images (AMI) et logiciel en tant que service (SaaS, Software as a Service). Pour plus d'informations sur les différents types de logiciels, consultezTypes de produit.

Pour vous aider à choisir le logiciel dont vous avez besoin,AWS Marketplacefournit les informations suivantes :

- Description du vendeur
- Version du logiciel
- Type de logiciel (AMI ou SaaS), ainsi que des informations sur l'AMI, le cas échéant
- Évaluation de l'acheteur
- Prix
- Informations sur le produit

Différences entre lesAWS Marketplaceet Amazon DevPay

Les différences entre les et lesAWS Marketplaceet Amazon DevPay. Les deux aident les clients à acheter des logiciels qui s'exécutentAWS, maisAWS Marketplaceoffre une expérience plus complète qu'Amazon DevPay. Pour les acheteurs de logiciels, les différences clés sont les suivantes :

- AWS Marketplaceoffre une expérience d'achat plus similaire à Amazon.com, en simplifiant la découverte des logiciels disponibles.
- AWS Marketplaceproduits fonctionnent avec d'autres produitsAWSnotamment les VPC, Private Cloud (VPC) et peuvent être exécutées sur des instances réservées et Spot Amazon Elastic Compute Cloud (Amazon EC2), outre des instances à la demande.
- AWS Marketplaceprend en charge les logiciels basés sur Amazon Elastic Block Store (Amazon EBS) et Amazon DevPay ne l'inclut pas.

En outre, les vendeurs de logiciels bénéficient de la promotion étendue et de la facilité de découverte deAWS Marketplace.

Débuter en tant qu'acheteur

Les rubriques suivantes décrivent la procédure à suivre pour démarrer avec des produits logiciels en tant qu'AWS Marketplaceacheteur.

Rubriques

Pour plus d'informations sur la prise en main des produits de données, consultez la section Abonnement à des produits de données sur AWS Data Exchange dans le guide de l'utilisateur d'AWS Data Exchange.

Achat de produits

DansAWS Marketplace, acheter un produit signifie que vous avez accepté les conditions du produit comme indiqué sur la page de mise en vente du produit. Cela inclut les conditions de tarification et le contrat de licence utilisateur final (CLUF) du vendeur, ainsi que le fait que vous acceptez d'utiliser ce produit conformément au contrat client AWS. Vous recevrez une notification par e-mail à l'adresse e-mail associée à votreCompte AWSpour les offres acceptées dansAWS Marketplace.

Si le produit a un coût mensuel ou est acheté avec un contrat d'abonnement, il vous sera facturé au prorata de l'abonnement. L'abonnement est calculé au prorata du temps restant dans le mois. Aucune autre charge n'est évaluée tant que vous n'effectuez pas l'une des actions suivantes :

- Lancez une instance Amazon Elastic Compute Cloud (Amazon EC2) avec le produit Amazon Machine Image (AMI).
- Déployez le produit en utilisant unAWS CloudFormationmodèle.
- Enregistrez le produit sur le site Web du vendeur.

Si le produit propose une option d'abonnement annuel, la totalité du paiement vous est facturée au moment de l'abonnement. Ce paiement couvre l'utilisation de base du produit, le renouvellement de l'abonnement ayant lieu à la date anniversaire du premier paiement. Si vous ne renouvelez pas à la

fin de la période d'abonnement annuelle, l'abonnement est converti en abonnement horaire au tarif horaire en cours.

Pour plus d'informations sur les abonnements aux produits de données, consultezAbonnement à des produits de données sur AWS Data Exchangedans leAWS Data Exchange Guide de l'utilisateur.

Lancement des logiciels

Après avoir acheté un logiciel, vous pouvez lancer les AMI (Amazon Machine Images) qui le contiennent à l'aide de la vue 1-Click Launch (Lancement en un clic) dans AWS Marketplace. Vous pouvez également le lancer à l'aide d'autres Amazon Web Services (AWS), y compris les outils de gestionAWS Management Console, la console Amazon Elastic Compute Cloud (Amazon EC2), les API d'Amazon EC2 ouAWS CloudFormationconsole

Avec l'1-Click Launch, vous pouvez vérifier et modifier rapidement, puis de lancer une seule instance du logiciel avec les paramètres recommandés par le vendeur du logiciel. LeLancer avec la console EC2constitue un moyen simple de trouver le numéro d'identification d'AMI et d'autres informations pertinentes qui sont nécessaires pour lancer l'AMI à l'aide de laAWS Management Console, les API Amazon EC2 ou d'autres outils de gestion. LeLancer avec la console EC2fournit également plus d'options de configuration que le lancement à partir de laAWS Management Console, comme le balisage d'une instance.

PourAWS Marketplaceproduits aux topologies complexes,Lancement personnaliséview fournit uneLancez avec CloudFormation Consolequi charge le produit dans le dossierAWS CloudFormationconsole avec la console appropriéeAWS CloudFormationmodèle Template. Vous pouvez ensuite suivre les étapes décrites dans la sectionAWS CloudFormationassistant de console pour créer le cluster d'AMI etAWSressources pour ce produit.

Tutoriel : Acheter un produit logiciel basé sur AMI

Le tutoriel suivant explique comment acheter un produit Amazon Machine Image (AMI) avecAWS Marketplace.

Étapes

- Étape 1 : Création d'unCompte AWS
- Étape 2 : Choix de votre logiciel
- Étape 3 : Configuration de votre logiciel
- Étape 4 : lancement de votre logiciel sur Amazon EC2

Étape 1 : Création d'unCompte AWS

Vous pouvez parcourir leAWS Marketplace site Web (https://aws.amazon.com/marketplace) sans être connecté à votre compteCompte AWS. Toutefois, vous devez vous connecter pour vous abonner à des produits ou les lancer.

Vous devez être connecté à votre compteCompte AWS pour accéder à laAWS Marketplace console. Pour plus d'informations sur la création d'unCompte AWS, consultez la section Création d'unCompte AWS dans le GuideAWS Account Management de référence.

Étape 2 : Choix de votre logiciel

Choisir vos logiciels

1. Accédez au AWS Marketplacesite Web.

   > **Note**
   >
   > Vous pouvez acheter, vous abonner et lancer de nouvelles instances depuis leAWS Marketplace site Web public, à l'adresse https://aws.amazon.com/marketplace, ou viaAWS Marketplace leAWS Management Console site https://console.aws.amazon.com/marketplace/home#/subscriptions.
   > Les expériences sur les deux sites sont similaires. Cette procédure utilise leAWS Marketplace site Web, mais note toute différence majeure lors de l'utilisation de la console.

2. Le volet Shop All Categories (Acheter dans toutes les catégories) contient la liste des catégories parmi lesquelles faire votre choix. Vous pouvez également choisir un logiciel présenté dans le volet central. Pour ce didacticiel, dans le volet Shop All Categories, sélectionnez Content Management.
3. Dans la liste de gestion de contenu, sélectionnez WordPressCertifié par Bitnami et Automattic.
4. Sur la page de description du produit, examinez les informations sur le produit. La page de description du produit comprend des informations supplémentaires, notamment :

   - Évaluation de l'acheteur

- Offre d'assistance
- Éléments principaux
- Description détaillée du produit
- Détails des prix pour chaque type d'instanceRégion AWS (pour les AMI)
- Ressources supplémentaires pour vous aider à démarrer

5. Choisissez Continue to Subscribe (Continuer pour s'abonner).
6. Si vous n'êtes pas déjà connecté, vous êtes invité à vous connecter àAWS Marketplace. Si vous en avez déjàCompte AWS, vous pouvez l'utiliser pour vous connecter à ce compte. Si vous n'en avez pas encoreCompte AWS, consultezÉtape 1 : Création d'unCompte AWS.
7. Lisez les conditions de l'offre Bitnami, puis choisissez Accepter le contrat pour accepter l'offre d'abonnement.
8. L'opération d'abonnement peut prendre un certain temps. Lorsque c'est le cas, vous recevez un e-mail concernant les conditions de l'abonnement, puis vous pouvez continuer. Choisissez Continuer vers la configuration pour configurer et lancer votre logiciel.

S'abonner à un produit implique l'acceptation des conditions générales du produit. Si le produit est soumis à des frais mensuels, les frais vous sont facturés lors de l'abonnement, qui sont calculés au prorata du temps restant dans le mois. Aucun autre frais ne sera facturé tant d'avoir lancé une instance Amazon Elastic Compute Cloud (Amazon EC2) avec l'AMI de votre choix.

> **Note**
>
> En tant qu'abonné à un produit, votre compte reçoit des e-mails lorsqu'une nouvelle version du logiciel auquel vous êtes abonné est publiée.

Étape 3 : Configuration de votre logiciel

Comme nous avons choisi le logiciel comme AMI, l'étape suivante consiste à configurer le logiciel, notamment en sélectionnant le mode de diffusion, la version etRégion AWS l'utilisation du logiciel.

Pour configurer votre logiciel

1. Sur la page Configurer ce logiciel, sélectionnez Amazon Machine Image (AMI) 64 bits (x86) comme mode de livraison.
2. Choisissez la dernière version disponible pour la version logicielle.

3. Choisissez la région dans laquelle vous souhaitez lancer le produit, par exemple USA Est (Virginie du Nord).

> **Note**
>
> Lorsque vous apportez des modifications à votre configuration, vous remarquerez peut-être que l'identifiant Ami en bas de l'écran est mis à jour. L'ID d'AMI se présente sous la forme ami-<identifier>, par exemple, *ami-123example456*. Chaque version de chaque produit de chaque région possède une AMI différente. Cet ID AMI vous permet de spécifier l'AMI correcte à utiliser lors du lancement du produit. L'alias Ami est un identifiant similaire qui est plus facile à utiliser dans le cadre de l'automatisation. Pour plus d'informations sur l'alias AMI, consultezUtilisation des alias AMI.

4. Sélectionnez Poursuivre le lancement.

Étape 4 : lancement de votre logiciel sur Amazon EC2

Avant de lancer votre instance Amazon EC2, vous devez décider si vous souhaitez la lancer avec 1-Click Launch ou si vous souhaitez la lancer à l'aide de la console Amazon EC2. Le lancement en un clic vous permet de démarrer rapidement grâce aux options par défaut recommandées, telles que les groupes de sécurité et les types d'instances. Avec le lancement en 1 clic, vous pouvez également consulter votre facture mensuelle estimée. Si vous préférez davantage d'options, comme le lancement dans un Amazon Virtual Private Cloud (Amazon VPC) ou vous pouvez utiliser des instances Spot, vous pouvez le lancer depuis la console Amazon EC2. Les procédures suivantes vous expliquent comment vous abonner au produit et lancer une instance EC2 à l'aide de 1-Click Launch ou de la console Amazon EC2.

Lancement sur Amazon EC2 à l'aide du lancement en 1 clic

Pour lancer sur Amazon EC2 à l'aide du lancement en 1 clic

1. Sur la page Lancer ce logiciel, choisissez Lancer depuis le site Web dans la liste déroulante Choisir une action, puis passez en revue les paramètres par défaut. Pour modifier l'un d'eux, effectuez l'une des opérations suivantes :

   - Dans la liste déroulante Type d'instance EC2, sélectionnez un type d'instance.
   - Dans les listes déroulantes Paramètres du VPC et Paramètres du sous-réseau, sélectionnez les paramètres réseau que vous souhaitez utiliser.

- Dans les paramètres du groupe de sécurité, choisissez un groupe de sécurité existant ou choisissez Créer un nouveau groupe en fonction des paramètres du vendeur pour accepter les paramètres par défaut. Pour de plus amples informations sur les groupes de sécurité, veuillez consulter Groupes de sécurité Amazon EC2 pour les instances Linux dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
- Déployez Key Pair (Paire de clés), puis choisissez une paire de clés existante, si vous en avez une. Si vous n'en avez pas, vous êtes key pair en créer une, vous êtes invité à en créer une. Pour en savoir plus sur les paires de clés Amazon EC2, consultez Paires de clés Amazon EC2.

2. Lorsque vous êtes satisfait de vos paramètres, sélectionnez Lancer.

   Votre nouvelle instance est lancée avec les logiciels WordPressCertified by Bitnami et Automattic qui s'y exécutent. À partir de là, vous pouvez consulter les détails de l'instance, créer une autre instance ou afficher toutes les instances de votre logiciel.

Lancement sur Amazon EC2 à l'aide de Launch with EC2 Console

Pour un lancement sur Amazon EC2 avec la console EC2

1. Sur la page Lancer sur EC2, choisissez la vue Lancer avec la console EC2, puis sélectionnez une version d'AMI dans la liste Sélectionner une version.
2. Vérifiez les Paramètres du pare-feu, les Instructions d'installations et les Notes de mise à jour, puis choisissez Launch with EC2 Console (Lancement avec la console EC2).
3. Dans la console EC2, lancez votre AMI à l'aide de l'assistant de demande d'instance. Suivez les instructions dans Mise en route avec les instances Linux Amazon EC2 pour naviguer dans l'assistant.

Étape 5 : Gestion de votre logiciel

À tout moment, vous pouvez gérer vos abonnements logiciels à l'aideAWS Marketplace de la page Gérer les abonnements de la AWS Marketplaceconsole.

Pour gérer vos logiciels

1. Accédez à la AWS Marketplaceconsole et choisissez Gérer les abonnements.
2. Sur la page Gérer les abonnements :

- Afficher le statut de votre instance par produit
- Afficher vos frais mensuels en cours
- Exécuter une nouvelle instance
- Afficher les profils de vendeur pour votre instance
- Gérez vos instances
- Définir un lien directement vers votre instance Amazon EC2, pour configurer votre logiciel

Étape 6 : mise hors service de votre instance

Une fois que vous avez décidé que vous n'avez plus besoin de l'instance, vous pouvez la résilier.

> **Note**
>
> Vous ne pouvez pas redémarrer une instance terminée. Toutefois, vous pouvez lancer des instances supplémentaires de la même AMI.

Pour mettre fin à une instance

1. Accédez à la AWS Marketplaceconsole et choisissez Gérer les abonnements.
2. Sur la page Gérer les abonnements, choisissez l'abonnement logiciel dont vous souhaitez résilier une instance, puis sélectionnez Gérer.
3. Sur la page d'abonnement spécifique, choisissez Afficher les instances dans la liste déroulante Actions.
4. Sélectionnez la région dans laquelle se trouve l'instance que vous souhaitez résilier. Cela ouvre la console Amazon EC2 et affiche les instances de cette région dans un nouvel onglet. Si nécessaire, vous pouvez revenir à cet onglet pour voir l'ID d'instance à fermer.
5. Dans la console Amazon EC2, choisissez l'ID d'instance pour ouvrir la page de détails de l'instance.
6. Dans la liste déroulante État de l'instance, choisissez Résilier l'instance.
7. Choisissez Résilier lorsque vous êtes invité à confirmer.

   La mise hors service dure quelques minutes.

Pour plus d'informations

Pour en savoir plus sur les catégories et les types de produits, consultez Catégories de produits et Types de produit.

Pour en savoir plus sur Amazon EC2, consultez la documentation du service sur Amazon Elastic Compute Cloud Documentation.

Pour en savoir plusAWS, consultez https://aws.amazon.com/.

Régions AWS prises en charge dans AWS Marketplace

Pour les produits logiciels, le vendeur choisit dans quels logiciels Régions AWS il souhaite mettre son logiciel à disposition, ainsi que les types d'instances. Nous recommandons de rendre les produits disponibles dans toutes les régions et sur tous les types d'instance pertinents. Le site Web AWS Marketplace est disponible dans le monde entier et prend en charge les régions suivantes :

- Amérique du Nord
  - USA Est (Ohio)
  - USA Est (Virginie du Nord)
  - USA Ouest (Californie du Nord)
  - US West (Oregon)
  - AWS GovCloud (USA Est)
  - AWS GovCloud (US-Ouest)
  - Canada (Centre)
  - Canada Ouest (Calgary)

- Afrique
  - Afrique (Le Cap)

- Amérique du Sud
  - Amérique du Sud (São Paulo)

- EMEA
  - Europe (Francfort)
  - Europe (Irlande)
  - Europe (Londres)
  - Europe (Milan)
  - Europe (Paris)
  - Europe (Espagne)
  - Europe (Stockholm)
  - Europe (Zurich)

- APAC
  - Asie-Pacifique (Hong Kong)
  - Asie-Pacifique (Hyderabad)
  - Asie-Pacifique (Jakarta)
  - Asie-Pacifique (Melbourne)
  - Asie-Pacifique (Mumbai)
  - Asie-Pacifique (Osaka)
  - Asia Pacific (Seoul)
  - Asie-Pacifique (Singapour)
  - Asie-Pacifique (Sydney)
  - Asia Pacific (Tokyo)

- Moyen-Orient
  - Israël (Tel Aviv)
  - Moyen-Orient (Bahreïn)
  - Moyen-Orient (EAU)

Pour plus d'informations sur les régions prises en charge pour les produits de données, consultez la section Points de terminaison et quotas AWS Data Exchange dans le manuel de référence AWS général.

Catégories de produits

LeAWS MarketplaceLe site Web comprend des catégories principales divisées en sous-catégories. Vous pouvez effectuer des recherches et appliquer des filtres en fonction des catégories et sous-catégories.

Rubriques

- Logiciels d'infrastructure
- DevOps
- Applications métier
- Machine Learning (apprentissage automatique)
- IoT
- Services professionnels
- Applications de bureau
- Produits de données
- Industries

Logiciels d'infrastructure

Les produits dans cette catégorie fournissent des solutions liées à l'infrastructure.

Backup &

Produits utilisés pour des solutions de stockage et de sauvegarde.

Data Analytics

Produits utilisés pour l'analyse des données.

Calcul haute performance

Produits de calcul haute performance.

Migration

Produits utilisés pour les projets de migration.

Infrastructure réseau

Produits utilisés pour créer des solutions de mise en réseau.

Systèmes d'exploitation

Systèmes d'exploitation Linux et Windows packagés.

Sécurité

Produits de sécurité pour votre infrastructure.

Stockage

Applications axées sur des rôles liés au stockage.

DevOps

Les produits de cette catégorie fournissent des outils destinés aux développeurs et aux équipes de développeurs.

Gestion du cycle de vie

Produits utilisés pour la mise en œuvre du logiciel

Développement d'applications

Produits utilisés pour le développement d'applications.

Serveurs d'applications

Serveurs utilisés pour le développement d'applications.

Piles d'applications

Piles utilisées pour le développement d'applications.

Intégration et livraison continues

Produits utilisés pour la CI/CD.

Infrastructure en tant que code

Produits utilisés pour les infrastructures.

Problèmes & suivi des bogues

Produits utilisés par les équipes de développeurs pour le suivi et la gestion des bogues informatiques.

Surveillance

Produits utilisés pour la surveillance des logiciels d'exploitation.

Analyse de journaux

Produits utilisés pour l'analyse de la journalisation et des journaux.

Contrôle du code source

Outils utilisés pour la gestion et la maintenance du contrôle du code source.

Test

Produits utilisés pour les tests automatisés des produits logiciels.

Applications métier

Les produits de cette catégorie vous aident à gérer votre activité.

Blockchain

Produits utilisés pour la blockchain.

Collaboration & productivité

Produits utilisés pour faciliter la collaboration dans votre entreprise.

Centre de contact

Produits utilisés pour la mise en œuvre des centres de contact dans votre organisation.

Gestion de contenu

Produits axés sur la gestion de contenu.

CRM

Outils axés sur la gestion de la relation client.

eCommerce

Produits qui fournissent des solutions de eCommerce.

eLearning

Produits qui fournissent des solutions d'apprentissage.

Ressources humaines

Produits utilisés pour la mise en œuvre des ressources humaines au sein de votre organisation.

Gestion métier

Produits utilisés pour la mise en œuvre de la gestion de votre organisation.

Informatique décisionnelle

Produits utilisés pour la mise en œuvre de l'informatique décisionnelle au sein de votre organisation.

Gestion de projet

Outils de gestion de projet.

Machine Learning (apprentissage automatique)

Les produits de cette catégorie fournissent des algorithmes d'apprentissage automatique et des packages de modèles qui fonctionnent avec Amazon SageMaker.

Solutions d'apprentissage automatique

Solutions d'apprentissage automatique.

Services d'étiquetage de données

Produits qui fournissent une capacité d'étiquetage des données.

Aide visuelle par ordinateur

Produits qui fournissent une capacité de vision par ordinateur.

Traitement du langage naturel

Produits qui fournissent une capacité de traitement du langage naturel.

Reconnaissance vocale

Produits qui fournissent la capacité de reconnaissance vocale.

Text

Produits qui fournissent la capacité d'apprentissage de texte. Les exemples incluent la mise en œuvre de l'identification, les noms et la reconnaissance d'entités, l'identification, la text-to-speechet la traduction.

Image

Produits qui fournissent la capacité d'analyse d'images. Les exemples incluent la 3D, le sous-titrage, la classification, la modification/le traitement, l'intégration/l'extraction de fonctionnalités, la génération, la grammaire/l'analyse, la reconnaissance d'écriture manuscrite, humains/visages, la détection d'objets, la segmentation/étiquetage de pixel et texte/OCR.

Vidéo

Produits qui fournissent la capacité d'analyse vidéo. Les exemples incluent la réidentification du locuteur, la synthèse, la synthèse, le mouvement, la synthèse, la synthèse, le mouvement, la synthèse, la synthèse, le mouvement, la synthèse, le mouvement, la synthèse, le suivi.

Audio

Produits qui fournissent la capacité d'analyse audio. Les exemples incluent l'identification du locuteur speech-to-text, l'identification de chansons et la segmentation.

Structurée

Produits qui fournissent la capacité d'analyse structurée. Les exemples incluent la classification, le clustering, la réduction de dimensionnalité, les modèles de factorisation, l'ingénierie des fonctions, le classement, la régression et la prévision des séries chronologiques.

IoT

Produits utilisés pour créer des solutions de mise en réseau liées à l'IoT.

Analyse

Produits d'analyse pour les solutions IoT.

Applications

Produits d'application pour les solutions IoT.

Connectivité des appareils

Produits utilisés pour gérer la connectivité des appareils.

Gestion des appareils

Produits utilisés pour gérer des appareils.

Sécurité des appareils

Produits utilisés pour gérer la sécurité de vos appareils IoT.

IoT industriel

Produits destinés à fournir des solutions liées à l'IoT industriel.

Maison et ville

Produits utilisés pour la mise en œuvre de solutions pour des maisons et des villes intelligentes.

Services professionnels

Les produits de cette catégorie fournissent des services de conseil liés àAWS MarketplaceProduits .

Évaluations

Évaluation de votre environnement d'exploitation actuel afin de trouver les solutions adaptées à votre organisation.

Mise en œuvre

Aide à la configuration, à la configuration et au déploiement de logiciels tiers.

Managed Services

End-to-end la gestion de l'environnement en votre nom.

Premium Support

Accès aux conseils et à l'assistance d'experts, conçus pour répondre à vos besoins.

Entrainement

Des ateliers, des programmes et des outils éducatifs personnalisés fournis par des experts pour aider vos employés à apprendre les meilleures pratiques.

Applications de bureau

Les produits dans cette catégorie fournissent des solutions liées à l'infrastructure.

Applications de bureau

Applications et utilitaires de bureau pour la productivité générale et la mise en œuvre de rôles spécifiques.

AP et facturation

Applications utilisées pour les rôles axés sur les comptes payants et la facturation.

Application et le Web

Applications à usage général et environnement Web.

Développement

Applications utilisées pour le développement.

Informatique décisionnelle

Applications utilisées par les rôles axées sur la gestion de l'informatique décisionnelle.

CAD et CAM

Applications utilisées par les rôles axées sur la conception et la fabrication assistées par ordinateur.

SIG et cartographie

Applications utilisées par les rôles axées sur les SIG et la cartographie.

Illustration et conception

Applications pour les rôles axées sur l'illustration et la conception.

Médias et codage

Application utilisée pour les rôles impliqués dans l'encodage et les médias.

Productivité et collaboration

Applications destinées à améliorer la productivité et la collaboration.

Gestion de projet

Application pour les rôles de gestion de projet.

Sécurité/Stockage/Archivage

Applications axées sur des rôles liés à la sécurité, au stockage et à l'archivage des données.

Utilitaires

Applications axées sur différents rôles.

Produits de données

Les produits de cette catégorie sont des ensembles de données basées sur des fichiers. Pour plus d'informations, consultez le .Guide de l'utilisateur d'AWS.

Industries

Éducation &

Produits visant à fournir des solutions pour la recherche et l'enseignement.

Services financiers

Produits pour la mise en œuvre de services financiers au sein de votre organisation.

Santé & sciences de la vie

Produits utilisés dans les secteurs de la santé et des sciences de la vie.

Médias &

Produits et solutions liés au contenu multimédia.

Industri

Produits et solutions liés au secteur.

Énergie

Produits et solutions liés à l'énergie.

Types de produit

AWS Marketplaceinclut des logiciels open source et commerciaux populaires, ainsi que des produits de données gratuits et payants. Ces produits sont disponibles de différentes manières : en tant que Amazon Machine Images (AMI) individuelles, en tant que cluster d'AMI déployées via un AWS CloudFormation modèle, en tant que logiciel en tant que service (SaaS), en tant que services professionnels et en tant que produits de données AWS Data Exchange.

Pour plus de détails sur ces types de produits, consultez les rubriques suivantes :

- Produits pour serveurs basés sur l'AMI(y compris AMI et produits d'image privée)
- Produits de conteneur
- Produits de Machine Learning
- Produits de services professionnels
- Produits SaaS
- Produits de données

Produits pour serveurs basés sur l'AMI

Une Amazon Machine Image (AMI) est une image d'un serveur, comprenant un système d'exploitation et souvent des logiciels supplémentaires, qui s'exécute surAWS.

Les logiciels répertoriés dansAWS Marketplaceest uniquement disponible pour être exécuté sur Amazon Elastic Compute Cloud (Amazon EC2). Il n'est pas disponible au téléchargement.

SurAWS Marketplace, vous pouvez rechercher des AMI (avec des suggestions de recherche), consulter les avis sur les produits soumis par d'autres clients, vous abonner et lancer des AMI, et gérer vos abonnements. ToutAWS Marketplacela qualité des produits a été vérifiée et préconfigurés pour être lancés en un clic sur Amazon Web Services (AWS) infrastructure.

Les listes de produits AMI et de logiciel en tant que service (SaaS) proviennent de vendeurs de confiance. Les produits AMI fonctionnent dans les limites de celles d'un clientCompte AWS. Vous disposez d'un plus grand contrôle sur la configuration du logiciel et sur les serveurs qui l'exécutent, mais vous avez également des responsabilités supplémentaires concernant la configuration et la maintenance du serveur.

LeAWS MarketplaceLe catalogue contient une sélection de logiciels open source et commerciaux de vendeurs renommés. De nombreux produits surAWS Marketplacepeuvent être achetés à l'heure.

Le catalogue d'AMI est une ressource communautaire où les personnes et les équipes de développement peuvent présenter et échanger des logiciels ou des projets en cours de développement, sans devoir les soumettre à des vérifications approfondies. Les offres du catalogue d'AMI de la communauté peuvent ou non être publiées par des vendeurs connus et n'ont pas fait l'objet de vérifications supplémentaires.

UnAWS Marketplacele produit contient une AMI pour chaqueRégion AWSdans lequel le produit est disponible. Ces AMI sont identiques à l'exception de leur emplacement. De plus, lorsque les vendeurs mettent à jour leur produit avec les derniers correctifs et mises à jour, ils peuvent ajouter un autre ensemble d'AMI au produit.

CertainsAWS Marketplaceles produits peuvent lancer plusieurs instances d'une AMI parce qu'ils sont déployés en tant que cluster à l'aide deAWS CloudFormationmodèles. Ce groupe d'instances, ainsi que d'autresAWSles services d'infrastructure configurés par leCloudFormationmodèle, agit comme un déploiement de produit unique.

Modèle AWS CloudFormation

> **Important**
>
> AWS Marketplacesupprimera le mode de livraison pour plusieurs produits Amazon Machine Image (AMI) en utilisantAWS CloudFormationmodèles en août 2024. AutresAWS Marketplaceproduits utilisantCloudFormation, par exemple une AMI unique avecCloudFormation, ne sera pas affecté.
> Jusqu'en août 2024, les abonnés existants peuvent lancer de nouvelles instances de leurs multiples produits AMI en utilisantCloudFormationmodèles deAWS Marketplace. Après l'arrêt, ils ne seront plus en mesure de lancer de nouvelles instances. Les instances existantes précédemment lancées et exécutées dans Amazon Elastic Compute Cloud (Amazon EC2) ne seront pas affectées et continueront de fonctionner.
> Si vous avez des questions, contactez AWS Support.

AWS CloudFormation est un service qui vous permet de modéliser et de configurer vos ressources AWS de sorte que vous puissiez passer moins de temps à gérer ces ressources et consacrer plus de temps à vos applications exécutées dans AWS. UNCloudFormationle modèle décrit

les différentsAWSles ressources que vous souhaitez, telles que les instances Amazon Elastic Compute Cloud (Amazon EC2) ou les instances de base de données Amazon Relational Database Service (Amazon RDS). CloudFormations'occupe du provisionnement et de la configuration de ces ressources pour vous. Pour plus d'informations, voirCommencer à utiliser AWSCloudFormation.

En utilisantAWS CloudFormationmodèles

Les vendeurs de logiciels peuvent proposerCloudFormationmodèles pour définir une topologie de déploiement préférée composée de plusieurs instances AMI et d'autresAWSressources. Si unCloudFormationun modèle est disponible pour un produit, il sera répertorié en tant qu'option de déploiement sur la page de liste des produits.

Vous pouvez utiliser une AMI pour déployer une seule instance Amazon EC2. Vous pouvez utiliser unCloudFormationmodèle pour déployer plusieurs instances d'une AMI agissant comme un cluster, ainsi queAWSdes ressources telles qu'Amazon RDS, Amazon Simple Storage Service (Amazon S3) ou toute autreAWSservice, sous la forme d'une solution unique.

Rubriques

- Abonnements AMI enAWS Marketplace
- Produits AMI avec tarification contractuelle
- Produits AMI activés pour le comptage
- Marquage de la répartition des coûts dans les produits AMI
- Création d'une image privée
- Utilisation des alias AMI

Abonnements AMI enAWS Marketplace

EnAWS Marketplace outre, certains produits logiciels basés sur Amazon Machine Image (AMI) proposent un modèle de tarification par abonnement annuel. Avec ce modèle de tarification, vous effectuez un paiement initial unique et vous ne payez aucun frais d'utilisation horaire pour les 12 prochains mois. Vous pouvez appliquer un abonnement annuel à un produitAWS Marketplace logiciel à une instance Amazon Elastic Compute Cloud (Amazon EC2).

> **Note**
>
> Pour les AMI horaires avec tarif annuel, l'abonnement annuel couvre uniquement les types d'instances que vous spécifiez lors de l'achat. Par exemple, `t3.medium`. Le lancement

de tout autre type d'instance entraînera le tarif horaire correspondant à ce type d'instance en fonction de l'abonnement actif. Vous ne pouvez pas modifier le type d'instance d'un abonnement annuel une fois qu'il a été acheté.

Vous pouvez également continuer à lancer et à exécuter des produitsAWS Marketplace logiciels en utilisant la tarification horaire. Les frais d'utilisation d'Amazon EC2 et des autres services proposés par AmazonAWS sont distincts et s'ajoutent à ceux que vous payez pour l'achat de produitsAWS Marketplace logiciels.

Si vous modifiez le type d'instance Amazon EC2 pour une utilisation horaire, votre infrastructure Amazon EC2 sera facturée conformément au plan d'épargne que vous avez signé. Toutefois, le formulaire de licence AMIAWS Marketplace sera automatiquement remplacé par un tarif horaire.

Si un produit horaire AMI ne prend pas en charge la tarification annuelle, l'acheteur ne peut pas acheter d'abonnement annuel. Si un produit horaire AMI prend en charge la tarification annuelle, l'acheteur peut accéder à la page du produitAWS Marketplace et acheter des contrats annuels. Chaque contrat annuel permet à l'acheteur de gérer une instance sans se voir facturer le tarif horaire. Les contrats varient en fonction du type d'instance.

Produits AMI avec tarification contractuelle

Certains vendeurs proposent des produits logiciels Amazon Machine Image (AMI) publics avec un modèle de tarification contractuel. Dans ce modèle, vous acceptez d'effectuer un paiement initial unique pour des quantités discrètes de licences afin d'accéder au produit logiciel pendant la durée de votre choix. Vous êtes facturé, à l'avance, par le biais de votreCompte AWS. Par exemple, vous pouvez acheter 10 licences d'accès utilisateur et 5 licences d'administration pour une année. Vous pouvez choisir de renouveler automatiquement les licences.

En outre, certaines entreprises proposent des produits logiciels privés basés sur des AMI avec un modèle de tarification contractuelle. Une offre privée a généralement une durée fixe que vous ne pouvez pas modifier.

Vous pouvez acheter un contrat de produit logiciel basé sur une AMI à travers la page détaillée du produit sur AWS Marketplace. Si cette option est disponible,AMI avec tarification contractuelleapparaît pourMéthode de remisesur la page détaillée du produit. Lorsque vous effectuez l'achat, vous serez dirigé vers le site Web du produit pour configurer un compte. Les frais d'utilisation apparaîtront alors sur votreCompte AWSrapport de facturation.

Abonnement à un produit AMI avec offre publique de tarification contractuelle

Pour souscrire à une offre publique d'un produit basé sur une AMI avec un modèle de tarification contractuelle

1. Connectez-vous àAWS Marketplaceet trouvez un produit logiciel basé sur des conteneurs avec un modèle de tarification contractuelle.
2. Dans la pageAbonnementsPage, afficher leInformations sur les prix.

   Vous trouverez ci-dessous leUnitéset le taux pour chaque durée (en mois).
3. ChoisissezContinuer à S'abonnerpour démarrer l'abonnement.

   Pour enregistrer ce produit sans vous abonner, choisissezEnregistrer dans la liste.
4. Créez un contrat en examinant les informations de tarification et en configurant les conditions du produit logiciel.

   a. Choisissez la durée du contrat :1 mois,12 mois,24 mois, ou36 mois

   b. UNDERParamètres de renouvellement, choisissez si vous souhaitez renouveler automatiquement le contrat.

   c. UNDEROptions de contrat, choisissez une quantité pour chaque unité.

   Le prix total du contrat est affiché sousInformations de tarification.
5. Une fois que vous avez effectué vos sélections, cliquez sur Create Contract (Créer contrat).

LePrix total contratest débité de votreCompte AWS. Une licence est générée dansAWS License Manager.

> **Note**
>
> Le traitement de l'abonnement et la génération d'une licence dans votreAWS License Managercompte pour le produit logiciel.

Abonnement à un produit AMI avec une offre privée de tarification contractuelle

Pour souscrire à une offre privée d'un produit basé sur une AMI avec un modèle de tarification contractuelle

1. Connectez-vous àAWS Marketplaceavec votre compte acheteur.
2. Affichage de l'offre privée.
3. Dans la pageAbonnementsPage, afficher leInformations sur les prix.

   Vous trouverez ci-dessous leUnitéset le taux pour chaque durée (en mois).
4. ChoisissezContinuer à S'abonnerpour démarrer l'abonnement.
5. Créez un contrat en examinant les informations de tarification et en configurant les conditions du produit logiciel.

   La durée du contrat est déjà fixée par le vendeur et ne peut pas être modifiée.
6. UNDEROptions de contrat, choisissez une quantité pour chaque unité.
7. Afficher le prix total du contrat sousInformations de tarification.

   Vous pouvez également consulter l'offre publique en choisissantAffichage de l'offresousAutres offres disponibles.
8. Une fois que vous avez effectué vos sélections, cliquez sur Create Contract (Créer contrat).

> **Note**
>
> Le traitement de l'abonnement et la génération d'une licence dans votreAWS License Managercompte pour le produit logiciel.

Accès au logiciel

Pour accéder au produit logiciel basé sur l'AMI

1. Dans la pageAWS Marketplaceconsole, accédez àAffichage de l'abonnementet consultez la licence du produit logiciel.
2. Dans la pageAbonnementsPage :

a. ChoisissezLicencepour consulter, accorder l'accès et suivre l'utilisation de vos droits dansAWS License Manager.

b. Choisissez Continuer vers Configuration.

3. Dans la pageLancement d', passez en revue votre configuration et choisissez la façon dont vous souhaitez lancer le logiciel sousAction.

4. Dans la pageChoisir un type d'instance, choisissez une instance Amazon Elastic Compute Cloud (Amazon EC2), puis choisissezSuivant: Configurer les détails d'instance.

5. Dans la pageConfigurer les détails d'instancePage, pourRôle IAMChoisissez un modèleAWS Identity and Access Management(IAM) depuis votreCompte AWS.

   Si vous n'avez pas de rôle IAM, choisissezCréation manuelle d'un nouveau rôle IAMlien et suivez les instructions.

> **Note**
>
> Lorsque vous achetez un produit avec un prix contractuel, une licence est créée parAWS Marketplacesur leCompte AWSque votre logiciel peut vérifier à l'aide de l'API License Manager. Vous aurez besoin d'un rôle IAM pour lancer une instance du produit basé sur l'AMI.
> Les autorisations IAM suivantes sont requises dans la stratégie IAM.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

6. Une fois les détails de l'instance configurés, choisissezExaminer et lancer.
7. Dans la pageExaminer le lancement d'instance, sélectionnez une key pair existante ou créez-en une autre, puis choisissezLancer des instances.

   LeLancement de lancements d'instancesUne fenêtre de progression s'affiche.
8. Une fois l'instance initiée, accédez au tableau de bord EC2, puis sousInstances, vérifiez que leÉtat de l'instanceafficheEn cours d'exécution.

Affichage d'une licence générée

Pour afficher une licence générée

1. Connectez-vous àAWS License Manageravec vos recettesCompte AWS.
2. UNDERLicense accordées, affichez toutes les licences que vous avez accordées.
3. Recherchez des licences en saisissant un SKU de produit, un destinataire ou un statut dans leRecherchebar.
4. Cliquez sur l'ongletID de licenceet afficher leInformations de licence.
5. Vous pouvez afficher leEmetteur(AWS/Marketplace) et leDroits(unités pour lesquelles la licence accorde le droit d'utiliser, d'accéder ou de consommer une application ou une ressource).

Modifier un contrat existant

S'ils ont déjà un engagement initial pour un produit AMI,AWS Marketplaceles acheteurs peuvent modifier certains aspects d'un contrat. Un contrat AMI est pris en charge par des offres basées sur les termes du contrat, par opposition aux offres de prix de consommation flexible (FCP) horaires ou annuels. Cette fonction est disponible uniquement pour les applications qui sont intégrées àAWS License Manager. Les acheteurs peuvent acheter des licences supplémentaires dans le cadre de la même offre dans le cadre du contrat en cours. Toutefois, les acheteurs ne peuvent pas réduire le nombre de droits achetés dans le contrat. Les acheteurs peuvent également annuler le renouvellement automatique de l'abonnement si l'option est activée par le vendeur.

> **Note**
>
> Une offre de contrat de calendrier de paiement flexible (FPS) ne peut pas être modifiée. Aucune modification des droits n'est disponible pour l'acheteur pour un contrat acheté par FPS. Un droit est un droit d'utiliser, d'accéder ou de consommer une application ou une ressource. Les offres FPS ne sont pas modifiables.

Gérer votre abonnement

1. Dans la pageAWS Marketplaceconsole, accédez àAffichage de l'abonnementet consultez la licence du produit logiciel.
2. Dans la pageAbonnementsPage SélectionnerLicence.
3. Dans la liste, sélectionnezAffichage des conditions générales.
4. DansOptions de contrat, augmentez vos droits à l'aide des flèches. Vous ne pouvez pas réduire le nombre de droits en dessous des droits achetés.
5. Les détails du contrat et le prix total s'affichent dans leInformations de tarificationSection.

Pour annuler le renouvellement automatique de votre abonnement

1. Dans la pageAWS Marketplaceconsole, accédez àAffichage de l'abonnementet consultez la licence du produit logiciel.
2. Dans la pageAbonnementsPage SélectionnerLicence.
3. Dans la pageAbonnement, recherchez leParamètres de renouvellementSection.
4. Assurez-vous de bien comprendre les termes et conditions d'annulation.
5. Cochez la case pour annuler le renouvellement automatique.

Produits AMI activés pour le comptage

Certains produits répertoriés sur AWS Marketplace sont facturés en fonction de l'utilisation mesurée par l'application logicielle. Parmi les exemples de dimensions d'utilisation mesurées, citons notamment les données d'utilisation, l'utilisation d'hôte/agent, ou l'utilisation de la bande passante. Pour fonctionner correctement, ces produits exigent une configuration supplémentaire. Au moment du test, un rôle IAM avec l'autorisation de mesurer l'utilisation doit être associé à

votreAWS MarketplaceAu moment du lancement, Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations sur les rôles IAM pour Amazon EC2, consultezRôles IAM pour Amazon EC2.

Marquage de la répartition des coûts dans les produits AMI

AWS Marketplaceprend en charge les balises de répartition des coûts pour les produits logiciels basés sur Amazon Machine Image (AMI). Les balises d'instance Amazon Elastic Compute Cloud (Amazon EC2) nouvelles et existantes sont automatiquement renseignées en fonction de l'utilisation de l'AWS MarketplaceAMI correspondante. Vous pouvez utiliser les balises de répartition des coûts activées pour identifier et suivre l'utilisation des AMI par le biaisAWS Cost Explorer des rapports deAWS coûts et d'utilisation,AWS des budgets ou d'autres outils d'analyse des dépenses cloud.

Le fournisseur qui a fourni l'AMI peut également enregistrer d'autres étiquettes personnalisées dans le compteur pour les produits basés sur l'AMI, sur la base d'informations spécifiques au produit. Pour en savoir plus, consultez Balisage de répartition des coûts.

Utilisez des balises pour organiser vos ressources et des balises de répartition des coûts pour effectuer le suivi de vos coûts AWS à un niveau détaillé. Une fois que ces balises sont activées, s'enAWS sert pour organiser les coûts de vos ressources dans votre rapport de répartition des coûts, afin de faciliter la catégorisation et le suivi de vosAWS coûts.

Le balisage de répartition des coûts s'en sert uniquement pour suivre les coûts à partir du moment où ces balises sont activées dans la console de Billing and Cost Management. SeulsCompte AWS les propriétaires, les propriétaires de comptes deAWS Organizations gestion et les utilisateurs disposant des autorisations appropriées peuvent accéder à la console de Billing and Cost Management d'un compte. Que vous utilisiez ou non le balisage de répartition des coûts, le montant qui vous est facturé reste inchangé. Le fait que vous utilisiez des balises de répartition des coûts n'a aucun impact sur les fonctionnalités de vos produits logiciels basés sur AMI.

Suivi des balises de répartition des coûts pour une AMI sur plusieurs instances

Chaque instance Amazon EC2 lancée pour un abonnementAWS Marketplace AMI est associée à une ligne d'utilisationAWS Marketplace logicielle correspondante dans le rapport sur lesAWS coûts et l'utilisation. VotreAWS Marketplace utilisation reflétera toujours les balises spécifiques appliquées à l'instance Amazon EC2 correspondante. Cela vous permet de distinguer vos coûts d'utilisation AWS Marketplace en fonction des différentes valeurs de balise qui ont été attribuées, au niveau de l'instance.

Vous pouvez également additionner vos coûts d'utilisation basés sur des balises pour qu'ils soient égaux aux frais d'utilisation du logiciel AMI reflétés dans votre facture à l'aide du Cost Explorer ou du rapportAWS Cost and Usage.

Recherche de budgets avec des instances balisées allouées aux coûts

Si vous avez déjà des budgets actifs filtrés en fonction des balises de répartition des coûts pour plusieurs instances Amazon EC2 dans la console de Billing and Cost Management, il peut être difficile de les trouver tous. Le script Python suivant renvoie une liste de budgets contenant des instances Amazon EC2 à partir deAWS Marketplace votre version actuelleRégion AWS.

Vous pouvez utiliser ce script pour connaître l'impact potentiel sur votre budget, ainsi que les cas dans lesquels des dépassements peuvent découler de cette modification. Notez que le montant facturé ne change pas, mais que la répartition des coûts sera reflétée plus précisément, ce qui peut avoir un impact sur les budgets.

```
#! /usr/bin/python

import boto3

session = boto3.Session()
b3account=boto3.client('sts').get_caller_identity()['Account']
print("using account {} in region {}".format(b3account,session.region_name))


def getBudgetFilters(filtertype):
    '''
    Returns budgets nested within the filter values [filter value][budeget name].
    The filtertype is the CostFilter Key such as Region, Service, TagKeyValue.
    '''
    budget_client = session.client('budgets')
    budgets_paginator = budget_client.get_paginator('describe_budgets')
    budget_result = budgets_paginator.paginate(
        AccountId=b3account
    ).build_full_result()
    returnval = {}
    if 'Budgets' in budget_result:
        for budget in budget_result['Budgets']:
            for cftype in budget['CostFilters']:
                if filtertype == cftype:
                    for cfval in budget['CostFilters'][cftype]:
                        if cfval in returnval:
```

```
                            if not budget['BudgetName'] in returnval[cfval]:
                                returnval[cfval].append(budget['BudgetName'])
                        else:
                            returnval[cfval] = [ budget['BudgetName'] ]
    return returnval

def getMarketplaceInstances():
    '''
    Get all the AWS EC2 instances which originated with AWS Marketplace.
    '''
    ec2_client = session.client('ec2')
    paginator = ec2_client.get_paginator('describe_instances')
    returnval = paginator.paginate(
        Filters=[{
            'Name': 'product-code.type',
            'Values': ['marketplace']
        }]
    ).build_full_result()
    return returnval


def getInstances():
    mp_instances = getMarketplaceInstances()
    budget_tags = getBudgetFilters("TagKeyValue")
    cost_instance_budgets = []
    for instance in [inst for resrv in mp_instances['Reservations'] for inst in
 resrv['Instances'] if 'Tags' in inst.keys()]:
        for tag in instance['Tags']:
            # combine the tag and value to get the budget filter string
            str_full = "user:{}${}".format(tag['Key'], tag['Value'])
            if str_full in budget_tags:
                for budget in budget_tags[str_full]:
                    if not budget in cost_instance_budgets:
                        cost_instance_budgets.append(budget)
    print("\r\nBudgets containing tagged Marketplace EC2 instances:")
    print( '\r\n'.join([budgetname for budgetname in cost_instance_budgets]) )


if __name__ == "__main__":
    getInstances()
```

Exemple de sortie

```
Using account 123456789012 in region us-east-2

Budgets containing tagged Marketplace EC2 instances:
EC2 simple
MP-test-2
```

Rubriques en relation

Pour plus d'informations, consultez les rubriques suivantes :

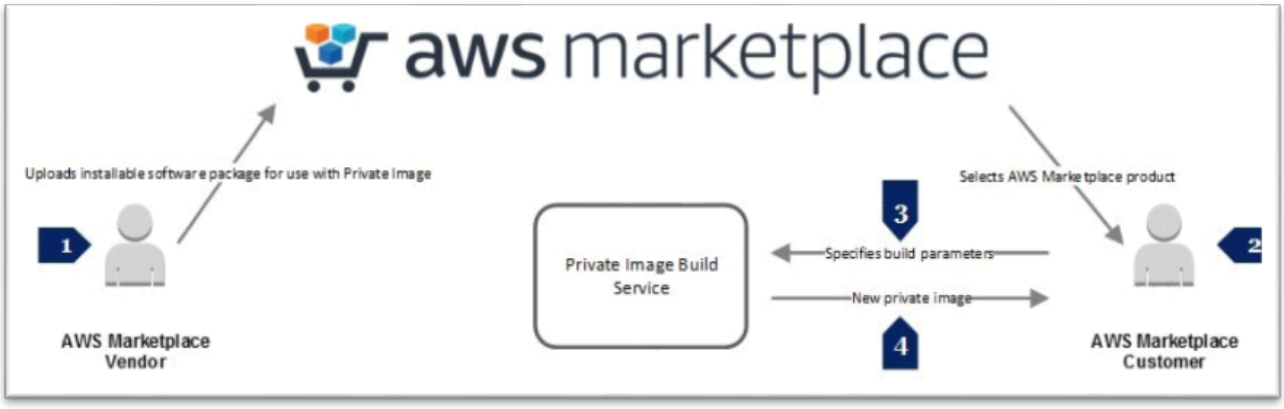
- Utilisation des balises de répartition des coûts dans le guide deAWS Billing l'utilisateur.
- Activation des balises de répartition des coûts générées par AWS dans le guide deAWS Billing l'utilisateur.
- Balisage de vos ressources Amazon EC2 dans le Guide de l'utilisateur pour les instances Linux Linux Linux Linux Linux Amazon EC2.

Création d'une image privée

> **Important**
>
> AWS Marketplaceinterrompra le mode de livraison Private Image Build en avril 2024. Jusqu'en avril 2024, les abonnés existants à Private Image Build peuvent créer de nouvelles Amazon Machine Images (AMI) dorées ou mettre à niveau leur AMI dorée à l'aide du logiciel fourni dans le mode de livraison Private Image Build. Après l'arrêt, ils ne seront plus en mesure de créer ou de mettre à niveau leur propre AMI à l'aide du logiciel Private Image Build. Les AMI existantes précédemment créées à l'aide de Private Image Build ne sont pas affectées. Cela signifie que les AMI créées à l'aide de Private Image Build peuvent continuer à être facturées et lancées à l'aide d'Amazon Elastic Compute Cloud (Amazon EC2) et que les instances actives continueront à s'exécuter comme elles le font aujourd'hui.
> En outre, les logiciels qui n'étaient auparavant disponibles que sous forme de génération d'image privée sont désormais disponibles via l'option autonome de traitement des AMI, qui ne sera pas abandonnée. L'AMI autonome peut toujours être utilisée avec votre abonnement Private Image Build existant après l'arrêt de Private Image Build. Si vous avez des questions, contactez AWS Support.

AWS MarketplacePrivate Image Build vous permet d'acheter des produits logiciels installables via,AWS Marketplace puis de les installer sur une image dorée ou une AMI que vous choisissez parmi les images disponibles sur votre compte AWS. Dans le cadre de ce document, une image renforcée est une image serveur qui inclut un système d'exploitation (OS) de base avec les modifications appliquées afin que chaque serveur lancé à partir de cette image respecte les normes informatiques que vous avez définies. Vous choisissez le logicielAWS Marketplace que vous souhaitez installer et l'AMI de base pour le build. Vous utilisez ensuite le serviceAWS Marketplace Image Build pour créer et diffuser une nouvelle AMI sous la forme d'une image privée disponible uniquement pour votre compte AWS.

Ce service vous aide à mieux répondre à vos exigences internes en matière de sécurité, de conformité et de gestion en vous permettant d'exécuterAWS Marketplace des produits sur un système d'exploitation de base conforme à vos normes informatiques.



Les vendeurs participant àAWS Marketplace Private Image Build créent des versions installables de leur produit pour des plateformes de système d'exploitation, des systèmes d'exploitation et des versions de système d'exploitation spécifiques. Lorsqu'un vendeur soumet un ensemble de packages logiciels pour son produit, le serviceAWS Marketplace Image Build installe et scanne le produit sur le système d'exploitation spécifié avant de le publierAWS Marketplace. Lorsque vous achetez un produit compatible avec la création d'imagesAWS Marketplace privées, vous pouvez choisir une AMI existante sur laquelle créer une nouvelle image privée. Une fois que vous avez utilisé le serviceAWS Marketplace Image Build pour créer une nouvelle image, celle-ci est disponible sur votre console Amazon EC2 en tant qu'image vous appartenant. Vous pouvez créer une image à l'aide duAWS Marketplace site Web ou utiliser l'APIAWS Marketplace Image Build Service.

Le logiciel et l'infrastructureServices AWS que vous utilisez pour terminer le processus de création sont payants, ce qui peut prendre de 1 à 2 heures selon le produit. Cependant, il n'y a pas de frais supplémentaires pour l'utilisation du serviceAWS Marketplace Image Build pour la création d'images

privées. Une fois l'image créée, aucun frais n'est facturé pour l'utilisation du produit ouAWS des ressources tant que vous n'utilisez pas le produit.

AWS MarketplacePrivate Image Build utilise AWS Identity and Access Management(IAM) pour créer des rôles et des politiques IAM qui accordent des autorisations limitées aux utilisateurs finaux pour créer et visualiser des images privées. La réalisation des étapes préalables exige des privilèges de niveau administratif.

Réalisation des étapes préalables

> **Important**
>
> AWS Marketplaceabandonnera le mode de livraison Private Image Build en avril 2024. Le mode de livraison n'est disponible que pour les abonnés existants jusqu'à son arrêt. Pour de plus amples informations, veuillez consulter Création d'une image privée.

Les étapes préalables décrites ici nécessitent des autorisations de niveau administratif qui configurent AWS Identity and Access Management (IAM) afin que vous puissiez accorder la possibilité de créer des images privées à d'autres utilisateurs. Une fois les politiques et les rôles IAM créés, vous pouvez les associer à des comptes de groupe (ou d'utilisateur) afin que les utilisateurs associés puissent créer des images privées.

IAM est un service web qui vous permet de contrôler l'accès aux AWS ressources. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources. Vous créez des identités (utilisateurs, groupes et rôles) et vous ajoutez les utilisateurs aux groupes, pour être ensuite en mesure de gérer des groupes plutôt que des utilisateurs individuels. Un rôle IAM est similaire à un utilisateur IAM, car il s'agit d'une identité avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dansAWS. En revanche, aucune information d'identification (mot de passe ou clés d'accès) n'est associée à celui-ci. Au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Un utilisateur peut endosser un rôle pour accepter différentes autorisations temporaires concernant un tâche spécifique.

La partie gestion des accès d'IAM vous aide à définir ce qu'un utilisateur ou une autre entité est autorisé à faire sur un compte, ce que l'on appelle souvent autorisation. Les autorisations sont accordées via des stratégies. Une politique est une entité dans AWS qui, lorsqu'elle est attachée à une identité ou à une ressource, définit les autorisations de cette dernière. AWS évalue ces politiques lorsqu'un principal, tel qu'un utilisateur, envoie une demande. Les autorisations dans les politiques

déterminent si la demande est autorisée ou refusée. Les stratégies sont stockées dans AWS sous forme de documents JSON attachés à des principaux en tant que stratégies basées sur l'identité, ou à des ressources en tant que stratégies basées sur les ressources. Vous accordez des autorisations en définissant des politiques d'autorisation et en attribuant la politique à un groupe.

Les stratégies basées sur l'identité sont des stratégies d'autorisation que vous pouvez attacher à un principal (ou une identité), comme un utilisateur, un rôle ou un groupe. Les stratégies basées sur les ressources sont des documents de stratégie JSON que vous attachez à une ressource, notamment un compartiment Amazon Simple Storage Service (Amazon S3). Les stratégies basées sur l'identité contrôlent les actions que peut effectuer cette identité, sur quelles ressources et dans quelles conditions. Les politiques basées sur l'identité peuvent être classées en politiques AWS gérées, politiques gérées par le client et politiques intégrées.

Les politiques basées sur les ressources contrôlent les actions qu'un principal spécifique peut effectuer sur cette ressource et dans quelles conditions. Les politiques basées sur les ressources sont des politiques en ligne et il n'y a pas de politiques basées sur des ressources gérées. Bien que les identités IAM soient techniquement AWS des ressources, vous ne pouvez pas associer de politique basée sur les ressources à une identité IAM. Vous devez utiliser des stratégies basées sur les identités dans IAM. Les politiques d'approbation sont des politiques basées sur des ressources qui sont attachées à un rôle et qui définissent les principaux qui peuvent endosser le rôle. Lorsque vous créez un rôle dans IAM, il doit inclure deux choses : une stratégie d'approbation qui indique qui peut assumer le rôle et une stratégie d'autorisation qui indique ce que cette personne peut faire avec ce rôle. Rappelez-vous qu'ajouter un compte à la stratégie d'approbation d'un rôle n'est qu'une partie de la procédure d'établissement de la relation d'approbation. Par défaut, aucun utilisateur des comptes approuvés ne peut assumer le rôle tant que l'administrateur de ce compte ne lui en a pas accordé l'autorisation.

Le service AWS Marketplace Image Building utilise deux rôles IAM, et chaque rôle dispose d'une politique d'autorisations et d'une politique de confiance. Si certains utilisateurs accèdent au AWS Marketplace site Web pour créer des images privées, ils ont également besoin d'autorisations IAM pour répertorier et attribuer les rôles nécessaires à la création et à l'affichage des images privées qu'ils créent.

En tant qu'administrateur, vous créez les deux rôles requis et leurs stratégies associées. Le premier rôle est un profil d'instance attaché à l'instance créée dans le cadre de la procédure de création d'image. Un profil d'instance est un conteneur pour un rôle IAM que vous pouvez utiliser pour transmettre les informations liées au rôle à une instance Amazon EC2 lorsque l'instance démarre. Le second est un rôle IAM qui fournit un accès à Amazon EC2 AWS Systems Manageret à Amazon

EC2. Pour configurer le profil d'instance, attachez une stratégie d'autorisation qui procure les autorisations exigées. Modifiez ensuite la stratégie d'approbation pour le rôle à autoriser Amazon EC2 et Systems Manager à assumer le rôle.

Création d'un rôle de profil d'instance

Pour créer le rôle de profil d'instance via la console IAM

1. Connectez-vous à l'outil AWS Management Console, puis ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Pour Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez Service AWS.
4. Dans Choisir le service qui utilisera ce rôle, choisissez EC2, puis Suivant : Autorisations.
5. Dans Créer une stratégie, choisissez Suivant : Examiner.
6. Dans Nom du rôle, saisissez un nom de rôle ou le suffixe d'un nom de rôle vous permettant d'identifier l'objectif du rôle, par exemple**`MyInstanceRole`**. Les noms de rôle doivent être uniques dans votreCompte AWS.
7. Passez en revue les informations du rôle, puis choisissez Créer un rôle.
8. Sur la page Rôles, sélectionnez le rôle que vous venez de créer.
9. Dans Autorisations, choisissez Ajouter une stratégie en ligne.
10. Choisissez l'onglet JSON et remplacez l'ensemble du texte par le `InstanceRolePermissionsPolicy` texte suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:GetDocument",
                "ssm:GetManifest",
                "ssm:GetParameters",
                "ssm:ListAssociations",
                "ssm:ListInstanceAssociations",
                "ssm:PutConfigurePackageResult",
                "ssm:UpdateAssociationStatus",
```

```
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2messages:AcknowledgeMessage",
                "ec2messages:DeleteMessage",
                "ec2messages:FailMessage",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ec2messages:SendReply"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Avant de commencer ce processus, vous devez créer le compartiment S3, *DOC-EXAMPLE-BUCKET*.

11. Choisissez Review policy (Examiner une politique).

12 Dans le champ Nom de la politique, entrez un nom qui vous aidera à identifier l'objectif de cette politique, par exemple**`MyInstanceRolePolicy`**, puis choisissez Créer une stratégie.

Pour modifier la relation d'approbation pour le rôle

1. Sur la page Rôles, sélectionnez le rôle que vous venez de créer.
2. Choisissez l'onglet Relations d'approbation, puis Modifier la relation d'approbation.
3. Sélectionnez tout le texte dans la zone de texte du document de politique et remplacez-le par le `InstanceRoleTrustPolicy` texte suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Choisissez Update Trust Policy (Mettre à jour la politique d'approbation).

Création d'un rôle AWS Systems Manager d'automatisation

Pour créer le rôle AWS Systems Manager d'automatisation

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
2. Pour Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez Service AWS.
3. Dans Choisir le service qui utilisera ce rôle, choisissez EC2, puis Suivant : Autorisations.
4. Dans Créer une stratégie, choisissez Suivant : Examiner.

5. Dans Nom du rôle, saisissez un nom de rôle ou le suffixe d'un nom de rôle vous permettant d'identifier l'objectif du rôle, par exemple**`MyAutomationRole`**. Les noms de rôle doivent être uniques dans votreCompte AWS.
6. Passez en revue les informations du rôle, puis choisissez Créer un rôle.
7. Sur la page Rôles, sélectionnez le rôle que vous venez de créer.
8. Dans Autorisations, choisissez Ajouter une stratégie en ligne.
9. Choisissez l'onglet JSON et remplacez tout le texte par le `AutomationRolePermissionsPolicy` texte suivant.

```
"Version": "2012-10-17",
"Statement": [
    {
        "Action": [
            "ssm:*"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:CreateImage",
            "ec2:DescribeImages",
            "ec2:StartInstances",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:CreateTags",
            "ec2:DescribeTags"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:PassRole"
```

```
            ],
            "Resource": [
                "{{ Instance Profile }}"
            ],
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Vous devez le `{{ Instance Profile }}` remplacer par l'Amazon Resource Name (ARN) du rôle de stratégie d'instance que vous avez créé précédemment. Localisez le rôle dans la console de gestion IAM et choisissez-le. Sur la page de résumé du rôle, le Role ARN est le premier élément répertorié, par exemple`arn:aws:iam::123456789012:role/MyInstanceRole`.

Pour modifier la relation d'approbation pour le rôle

1. Sur la page Rôles, sélectionnez le rôle que vous venez de créer.
2. Choisissez l'onglet Relations d'approbation, puis Modifier la relation d'approbation.
3. Remplacez tout le texte de la zone de texte du document de politique par le `InstanceRoleTrustPolicy` texte suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Choisissez Update Trust Policy (Mettre à jour la politique d'approbation).

Vous avez désormais créé les deux rôles et stratégies associées que vous utiliserez au cours du processus de création de l'image privée.

Utilisation d'une politique pour accéder au AWS Marketplace site Web

La plupart des entreprises n'autorisent pas les utilisateurs à se connecter à l'aide des informations d'identification du compte root. Au lieu de cela, ils créent des utilisateurs avec des autorisations limitées en fonction de rôles organisationnels ou de tâches que seules certaines personnes peuvent effectuer. AWS Marketplacefournit deux politiques principales gérées par IAM pour l'utilisation des AWS Marketplace outils. Utilisez ces deux stratégies gérées pour permettre la réalisation des tâches décrites :

- `AWSMarketplaceFullAccess`— Permet de s'abonner et de se désabonner du logiciel IAM, permet aux utilisateurs de gérer les instances AWS Marketplace logicielles depuis la page AWS Marketplace Votre logiciel et fournit un accès administratif à Amazon EC2.
- `AWSMarketplaceRead-only`— Permet de consulter les AWS abonnements.

Vous pouvez ajouter la politique `AWSMarketplaceFullAccess` gérée à un utilisateur, à un groupe ou à un rôle afin de fournir toutes les autorisations nécessaires pour accéder au AWS Marketplace site Web et effectuer les tâches associées à AWS Marketplace Private Image Build.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.

- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

La prochaine fois qu'un utilisateur ou un membre d'un groupe ou d'un rôle que vous avez sélectionné accédera au AWS Marketplace site Web, il pourra effectuer les tâches associées au processus de création d'images privées.

Création d'une image privée

> **Important**
>
> AWS Marketplaceabandonnera le mode de livraison Private Image Build en avril 2024. Le mode de livraison n'est disponible que pour les abonnés existants jusqu'à son arrêt. Pour de plus amples informations, veuillez consulter Création d'image privée.

Lorsque vous créez une image privée, vous sélectionnez le package logiciel AWS Marketplace et l'image machine Amazon (AMI) de base dans votre console Amazon Elastic Compute Cloud (Amazon EC2) que vous utiliserez pour créer la nouvelle image privée. Avant de démarrer le processus de génération, vous devez configurer votre AWS environnement de manière à pouvoir fournir :

- L'ID AMI de l'image de base sur laquelle vous allez installer le AWS Marketplace produit.
- Nom du compartiment Amazon Simple Storage Service (Amazon S3) dans lequel stocker les journaux de build. Le compartiment S3 doit se trouver dans le compartiment dans Région AWS lequel l'AMI sera disponible.
- Le profil d'instance Amazon EC2 avec lequel le package sera installé (voir la section précédente).
- Le rôle d'automatisation AWS Identity and Access Management (IAM) que le processus de création d'image utilisera pour créer l'AMI (voir la section précédente).
- Nom de la nouvelle image privée.

Si vous avez de l'expérience en la matièreServices AWS, vous savez probablement comment choisirRégions AWS, trouver l'ID AMI sur votre tableau de bord Amazon EC2 et utiliser les compartiments Amazon S3.

Pour trouver un produit qui permet de créer une image privée, accédez à la page de recherche AWS Marketplace du produit et, pour le filtre de recherche du mode de livraison, choisissez Image privée d'une machine Amazon. À partir de la page de description du produit, configurez l'achat, la configuration et les options de distribution. Le produit que vous créez est ajouté à votreCompte AWS.

Outre les prérequis spécifiés dans la section précédente, votre AMI de base doit répondre aux exigences suivantes :

- LinuxLes AMI doivent avoir l'un `Wget` ou l'autre `cURL` installé et configuré. Windows Les AMI doivent être PowerShell installées.
- LinuxLes AMI doivent être capables d'exécuter des scripts de données utilisateur EC2 ou disposer de l'AWS Systems Manageragent (agent SSM) préinstallé.
- WindowsL'agent SSM doit être préinstallé sur les AMI.

Pour créer une image privée

1. Sur AWS Marketplacela page détaillée du produit, sélectionnez Continuer à m'abonner.
2. Sur la page S'abonner à ce logiciel, dans les Conditions générales, choisissez Afficher les détails pour voir le type d'instance, les coûts d'utilisation du logiciel et le contrat de licence de l'utilisateur final (CLUF) du produit. En fonction du produit, plusieurs types d'abonnements peuvent être proposés. Après avoir choisi le type d'abonnement, choisissez Accepter les conditions.
3. Choisissez Continue to Configuration (Continuer vers Configuration).
4. Sur la page Configurer ce logiciel, pour Option de distribution, choisissez Private Amazon Machine Image.
5. Dans la section Image privée, pour 1. Choisissez une région, choisissez votre région. Pour 2 Choisissez une image privée à lancer, puis choisissez Créer une nouvelle image privée.
6. Dans la section Créer une nouvelle image privée, dans Sélectionnez une AMI de base à utiliser, choisissez M'appartenant, Images publiques ou Images privées.
   a. Appartenant à moi : AMI qui appartiennent spécifiquement à votre Compte AWS
   b. image publique : AMI qui ont été partagées avec tous Comptes AWS
   c. image privée : AMI qui ont été partagées avec votre Compte AWS
7. Pour saisir l'ID AMI de base publique ou Entrer l'ID AMI de base privée, entrez l'ID AMI ou utilisez la console Amazon EC2 pour copier-coller l'ID AMI de l'image que vous souhaitez utiliser comme AMI de base.

8. Dans Profil d'instance, choisissez le rôle de l'instance que vous avez créée en tant que condition préalable.
9. Dans Rôle d'automatisation, choisissez le rôle d'automatisation que vous avez créé en tant que condition préalable.
10. Dans Journaux de création, saisissez le nom d'un compartiment Amazon S3 où vous souhaitez stocker les journaux. Il s'agit du nom du bucket simple, par exemple *DOC-EXAMPLE-BUCKET*, plutôt que du nom DNS complet.
11. Dans Nom de l'image privée, saisissez le nom de la nouvelle image privée.

Nous vous recommandons d'utiliser une convention de dénomination pour les images privées que vous créez afin de faciliter leur identification. De plus, lorsque le service de création d'AWS Marketplaceimages crée une nouvelle image privée, il ajoute une AWSMarketplacebalise FulfillmentID, qui peut être utile pour identifier ultérieurement vos images privées. Vous pouvez également effectuer les étapes facultatives suivantes pour fournir des détails supplémentaires ou démarrer le processus de création en choisissant Start Build (Démarrer la création).

(Facultatif) Pour fournir des détails supplémentaires sur l'image privée

1. Pour les notes de description, entrez toutes les informations pertinentes que vous souhaitez inclure pour l'instance qui sera utilisée lors de la création de l'image privée.
2. Dans Type d'instance, choisissez le type d'instance que vous souhaitez utiliser lors de la création de l'image privée.
3. Dans VPC, choisissez le VPC que vous voulez que l'instance utilise lors de la création de l'image privée, puis choisissez le groupe de sécurité et le sous-réseau.
4. Dans Enable Simple Notification System, choisissez une rubrique existante ou créez une nouvelle rubrique pour recevoir des notifications lorsque le statut de la création change.
5. Choisissez Démarrer la création.

Le processus de création prend 1 à 2 heures. Notez les informations suivantes concernant le processus :

- Les frais des services utilisés pendant le processus de création apparaîtront dans le champ Compte AWS utilisé pour démarrer le processus de création de l'image privée. Cela inclut l'instance qui s'exécute pendant l'installation AWS Marketplace du produit sur l'image privée et le compartiment S3 utilisé pour les journaux.

- Vous pouvez voir l'état du processus de création ou recevoir des messages Amazon Simple Notification Service (Amazon SNS).
- Une fois la création terminée, la nouvelle image privée est ajoutée à votre Compte AWS et est disponible via la console Amazon EC2 en tant qu'AMI répertoriée sous la rubrique Appartenant à moi.
- Les référentiels utilisés pour terminer le processus de création doivent être locaux.
- Pendant la construction, le processus bloque l'accès à Internet.

Utilisation des alias AMI

Une Amazon Machine Image (AMI) est identifiée par un`AMI ID`. Vous pouvez utiliser le plugin`AMI ID`pour indiquer l'AMI que vous souhaitez utiliser lorsque vous lancez un produit. Le`AMI ID`Comporte le formulaire`ami-<identifier>`par exemple,ami-123 exemple 456. Chaque version de chaque produit dans chaqueRégion AWSpossède une AMI différente (et`AMI ID`).

Lorsque vous lancez un produit à partirAWS Marketplace, le`AMI ID`Est automatiquement renseigné pour vous. HAVING`AMI ID`Est utile si vous souhaitez automatiser le lancement de produits depuisAWS Command Line Interface(AWS CLI) ou en utilisant Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez trouver le`AMI ID`lorsque vous configurez votre logiciel au moment du lancement. Pour plus d'informations, consultez Étape 3 : Configuration de votre logiciel.

Le`Ami Alias`est également dans le même emplacement que le`AMI ID`, lors de la configuration de votre logiciel. Le`Ami Alias`est un identifiant similaire à celui de`AMI ID`, mais il est plus facile à utiliser dans l'automatisation. Un`AMI alias`Comporte le formulaire`aws/service/marketplace/prod-<identifier>/<version>`par exemple, `aws/service/marketplace/prod-1234example5678/12.2`. Vous pouvez utiliser cette`Ami Alias`ID dans n'importe quelle région, etAWSle met automatiquement en correspondance avec la bonne région`AMI ID`.

Si vous souhaitez utiliser la version la plus récente d'un produit, utilisez le terme**`latest`**à la place de la version dans`AMI alias`tel est le casAWSchoisit la version la plus récente du produit pour vous, par exemple,**`aws/service/marketplace/prod-1234example5678/latest`**.

> **Warning**
>
> Utilisation de**`latest`**vous permet de connaître la version la plus récente du logiciel. Toutefois, utilisez cette fonction avec prudence. Par exemple, si les versions 1.x et 2.x

d'un produit sont disponibles, il se peut que vous utilisiez 2.x. Cependant, la version la plus récente du produit peut être une correction de bogue pour la version 1.x.

Exemples d'utilisation d'alias d'AMI

Les alias d'AMI sont utiles pour l'automatisation. Vous pouvez les utiliser dans leAWS CLIou dansAWS CloudFormationModèles.

L'exemple suivant montre l'utilisation d'un alias AMI pour lancer une instance à l'aide deAWS CLI.

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
--instance-type m5.xlarge
--key-name MyKeyPair
```

L'exemple suivant présente un CloudFormation qui accepte l'alias d'AMI en tant que paramètre d'entrée pour créer une instance.

```
AWSTemplateFormatVersion: 2010-09-09

Parameters:
    AmiAlias:
        Description: AMI alias
        Type: 'String'

Resources:
    MyEC2Instance:
        Type: AWS::EC2::Instance
        Properties:
            ImageId: !Sub "resolve:ssm:${AmiAlias}"
            InstanceType: "g4dn.xlarge"
            Tags:
                -Key: "Created from"
                 Value: !Ref AmiAlias
```

Produits de conteneur

Les produits en conteneur sont des produits autonomes fournis sous forme d'images de conteneurs. Les produits en conteneur peuvent être gratuits ou doivent être payés à l'aide d'une option de

tarification proposée par le vendeur. Les produits de conteneurs peuvent être utilisés avec plusieurs environnements d'exécution et services de conteneur, notamment Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) et même des services exécutés sur votre propre infrastructure. Pour obtenir la liste complète des environnements d'exécution et des services pris en charge avec plus d'informations sur chacun d'entre eux, consultezServices pris en charge pour les produits en conteneur.

Vous pouvez découvrir des produits conteneurisés, vous y abonner et les déployer sur le AWS Marketplace site Web ou dans la console Amazon ECS. Vous pouvez déployer de nombreux produits sur Amazon ECS ou Amazon EKS à l'aide de modèles de déploiement fournis par le vendeur, tels que des définitions de tâches ou des diagrammes Helm. Vous pouvez également accéder aux images de conteneurs directement depuis les référentiels privés Amazon Elastic Container Registry (Amazon ECR) une fois que vous vous êtes abonné à ces produits.

Si un produit est activé QuickLaunch, vous pouvez l'utiliser pour tester rapidement des produits en conteneur sur un cluster Amazon EKS en quelques étapes seulement. QuickLaunch permet AWS CloudFormation de créer un cluster Amazon EKS et d'y lancer un logiciel de conteneur. Pour plus d'informations sur le lancement avec QuickLaunch, consultezQuickLaunch dans AWS Marketplace.

Cette section fournit des informations sur la recherche, l'abonnement et le lancement de produits conteneurisés dansAWS Marketplace.

Modèles de tarification pour les produits en conteneur payants

Les produits en conteneur payants doivent avoir un ou plusieurs modèles de tarification. Comme pour tous les autres produits payantsAWS Marketplace, les produits en conteneur payants vous sont facturés AWS conformément au modèle de tarification. Le modèle de tarification peut être un tarif mensuel fixe ou un prix horaire, contrôlé en quelques secondes et calculé au prorata. Les détails de la tarification seront affichés sur la page détaillée et lorsque vous vous abonnerez au produit.

Les modèles de tarification pris en charge pour les produits en conteneur AWS Marketplace sont les suivants :

- Des frais mensuels fixes qui permettent une utilisation illimitée.
- Des frais initiaux pour l'utilisation du produit pendant la durée d'un contrat à long terme.
- Un pay-as-you-go modèle (généralement horaire) basé sur l'utilisation du produit.
- Un pay-up-front modèle avec des prix contractuels.

Pour plus d'informations sur chaque modèle, consultez la section Tarification des produits Container dans le Guide du AWS Marketplace vendeur.

Présentation des conteneurs et de Kubernetes

Les conteneurs, tels que les conteneurs Docker, sont une technologie logicielle open source qui fournit une couche supplémentaire d'abstraction et d'automatisation par rapport aux systèmes d'exploitation virtualisés tels que Linux et Windows Server. Tout comme des machines virtuelles sont des instances d'images de serveur, les conteneurs sont des instances d'images de conteneur Docker. Ils intègrent des logiciels d'application serveur dans un système de fichiers qui contient tous les éléments nécessaires pour fonctionner : code, exécution, outils système, bibliothèques système, etc. Avec les conteneurs, le logiciel fonctionne toujours de la même manière, quel que soit son environnement.

À l'instar des machines virtuelles Java, les conteneurs nécessitent une plate-forme sous-jacente pour fournir une couche de traduction et d'orchestration tout en restant isolés du système d'exploitation et les uns des autres. Il existe différents environnements d'exécution et services d'orchestration compatibles avec Docker que vous pouvez utiliser avec les conteneurs Docker, notamment Amazon ECS, qui est un service d'orchestration hautement évolutif et performant, et Amazon EKS, qui facilite le déploiementAWS, la gestion et le dimensionnement d'applications conteneurisées à l'aide de Kubernetes, un service de gestion et d'orchestration open source.

Rechercher et s'abonner à des produits de conteneur

Les produits en conteneur sont des produits AWS Marketplace qui peuvent être lancés sur des images de conteneurs. Les produits en conteneur incluent tout produit AWS Marketplace dans lequel le vendeur a fourni une option d'expédition avec une image du conteneur, un tableau de bord ou un module complémentaire pour le mode de livraison Amazon EKS. Pour plus d'informations sur les méthodes de livraison des produits en conteneur, consultezModes de livraison des produits en conteneur.

De nombreux environnements de lancement, également appelés services pris en charge, sont disponibles pour les options d'expédition des produits en conteneur. Les environnements de lancement incluent des services tels qu'Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) et même votre propre infrastructure autogérée. Pour obtenir la liste complète des environnements de lancement de produits conteneurisés disponibles, consultezServices pris en charge pour les produits en conteneur.

Parcourez les produits en conteneur à l'aide du AWS Marketplace site Web

Vous pouvez parcourir les produits en conteneur en utilisant le AWS Marketplacesite Web.

Pour parcourir les produits en conteneur à l'aide du AWS Marketplace site Web

1. Accédez à la page AWS Marketplace de recherche.
2. Filtrez le mode de livraison par image du conteneur ou graphique Helm.
3. (Facultatif) Filtrez les services pris en charge pour affiner les résultats de recherche en fonction des services avec lesquels le produit peut être lancé.

Une fois que vous avez trouvé un produit qui vous intéresse, choisissez le titre pour accéder à la page de détails du produit.

Page détaillée du produit contenant

Sur la page de détails du produitAWS Marketplace, vous trouverez des informations sur le produit, notamment les informations suivantes :

- Aperçu du produit — L'aperçu comprend une description du produit et les informations suivantes :
  - Version du produit que vous êtes en train de consulter.
  - Lien vers le profil du vendeur.
  - Les catégories de produits auxquelles appartient ce produit.
  - Les systèmes d'exploitation pris en charge pour exécuter ce logiciel.
  - Les méthodes de livraison disponibles pour le lancement du logiciel.
  - Les services pris en charge sur lesquels ce produit peut être lancé.
- Informations sur les prix — Les produits proposent des niveaux gratuits, une licence Bring Your Own (BYOL), pay-up-front des prix contractuels, un prix mensuel ou annuel fixe, ou un prix horaire. pay-as-you-go Pour plus d'informations sur les modèles de tarification, consultez la section Tarification des produits Container.
- Informations d'utilisation : vous trouverez ici les options d'expédition fournies par le vendeur, ainsi que les instructions de lancement et d'exécution du logiciel. Chaque produit doit avoir au moins une option d'expédition et peut en avoir jusqu'à cinq. Chaque option d'expédition inclut un mode de livraison et des instructions à suivre pour lancer et exécuter le logiciel.
- Informations de support — Cette section contient des informations sur la manière d'obtenir de l'assistance pour le produit et sur sa politique de remboursement.

- Avis des clients — Trouvez les avis d'autres clients sur le produit ou rédigez les vôtres.

Pour vous abonner à un produit, choisissez Continuer à vous abonner sur la page de détails du produit. Pour plus d'informations sur l'abonnement aux produits, consultezAbonnement à des produits dans AWS Marketplace.

Abonnement à des produits dans AWS Marketplace

Pour utiliser un produit, vous devez d'abord vous y abonner. Sur la page d'abonnement, vous pouvez consulter les informations tarifaires des produits payants et accéder au contrat de licence utilisateur final (EULA) du logiciel.

Pour un produit dont le prix est contractuel par conteneur, sélectionnez le prix de votre contrat et choisissez Accepter le contrat pour continuer. Cela crée un abonnement au produit, qui donne le droit d'utiliser le logiciel. Le souscription de l'abonnement prend quelques minutes seulement. Une fois que vous aurez reçu le droit à un produit payant, vous serez débité lorsque vous commencerez à utiliser le logiciel. Si vous résiliez votre abonnement sans fermer toutes les instances en cours d'exécution, vous serez tout de même facturé pour tous les logiciels utilisés. Vous pouvez également avoir à payer des frais d'infrastructure liés à l'utilisation du produit. Par exemple, si vous créez un nouveau cluster Amazon EKS pour héberger le logiciel, vous serez facturé pour ce service.

> **Note**
>
> Pour découvrir comment s'abonner à un produit basé sur un conteneur et le déployer, vous pouvez également consulter les vidéos suivantes :
>
> - Déploiement de AWS Marketplace conteneurs sur des clusters Amazon ECS (3:34)
> - Déploiement de produits AWS Marketplace basés sur des conteneurs à l'aide d'Amazon ECS Anywhere (5:07)
> - Gestion des modules complémentaires Amazon EKS

Modes de livraison des produits en conteneur

Un produit AWS Marketplace est considéré comme un produit en conteneur si le vendeur a fourni au moins une option d'expédition avec une image du conteneur, un tableau de bord ou un module complémentaire pour le mode de livraison Amazon EKS.

Méthode de livraison des images du conteneur

Pour une option d'expédition avec une méthode de livraison d'images Container, utilisez les instructions fournies par le vendeur pour lancer le produit. Pour ce faire, les images Docker sont extraites directement du AWS Marketplace registre sur Amazon Elastic Container Registry. Pour plus d'informations sur le lancement avec ce mode de livraison, consultezLancement avec une option de traitement des images du conteneur.

Mode de livraison du Helm Chart

Pour une option d'expédition avec une méthode de livraison basée sur un plan Helm, utilisez les instructions ou le modèle de déploiement fournis par le vendeur pour lancer le produit. Cela se fait en installant un graphique Helm à l'aide de la CLI Helm. Vous pouvez lancer l'application sur un cluster Amazon EKS existant, sur un cluster autogéré sur EKS Anywhere Amazon Elastic Compute Cloud (Amazon EC2) ou sur site. Pour plus d'informations sur le lancement avec ce mode de livraison, consultezLancement avec une option Helm Fulfillment.

Module complémentaire pour le mode de livraison Amazon EKS

Pour une option d'exécution avec un module complémentaire pour le mode de livraison Amazon EKS, utilisez la console Amazon EKS ou la CLI Amazon EKS pour lancer le produit. Pour plus d'informations sur les modules complémentaires Amazon EKS, consultez les modules complémentaires Amazon EKS.

Services pris en charge pour les produits en conteneur

La liste suivante inclut tous les services pris en charge pour les produits en conteneur dansAWS Marketplace. Un service pris en charge est un service de conteneur ou un environnement dans lequel le produit peut être lancé. Un produit en conteneur doit inclure au moins une option d'expédition comprenant un mode de livraison avec des instructions de lancement vers un ou plusieurs environnements.

Amazon ECS

Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif que vous pouvez utiliser pour exécuter, arrêter et gérer des conteneurs sur un cluster. Vos conteneurs sont définis dans une définition de tâche qui vous sert à exécuter des tâches individuelles ou des tâches dans un service. Dans ce contexte, un service est une configuration qui permet d'exécuter et de gérer simultanément un certain nombre de tâches dans un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate.

Sinon, pour mieux contrôler votre infrastructure, vous pouvez exécuter vos tâches et services sur un cluster d'instances Amazon EC2 que vous gérez.

Pour plus d'informations sur Amazon ECS, consultez Qu'est-ce qu'Amazon Elastic Container Service dans le guide du développeur Amazon Elastic Container Service.

Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré que vous pouvez utiliser pour exécuter Kubernetes sur AWS sans avoir à installer, à utiliser et à entretenir vos propres plan de contrôle ou nœuds Kubernetes. Kubernetes est un système open source destiné à l'automatisation du déploiement, la mise à l'échelle et la gestion d'applications conteneurisées.

Vous pouvez rechercher des logiciels Kubernetes tiers, vous y abonner et les déployer à l'aide de la console Amazon EKS. Pour plus d'informations, consultez la section Gestion des modules complémentaires Amazon EKS dans le guide de l'utilisateur Amazon EKS.

Kubernetes autogéré

Vous pouvez lancer des produits conteneurisés sur des clusters Kubernetes autogérés exécutés dans Amazon ECSEKS Anywhere, Amazon Anywhere EC2 ou sur une infrastructure sur site.

Amazon ECS Anywhere est une fonctionnalité d'Amazon ECS que vous pouvez utiliser pour exécuter et gérer les charges de travail des conteneurs sur une infrastructure gérée par le client. Amazon ECS Anywhere s'appuie sur Amazon ECS pour fournir une expérience d'outillage et d'API cohérente pour toutes vos applications basées sur des conteneurs.

Pour plus d'informations, consultez Amazon ECS Anywhere.

EKS Anywhereest un service que vous pouvez utiliser pour créer un cluster Amazon EKS sur une infrastructure gérée par le client. Vous pouvez effectuer un déploiement EKS Anywhere en tant qu'environnement local non pris en charge ou en tant qu'environnement de production pouvant devenir une plate-forme Kubernetes sur site prise en charge.

Pour plus d'informations sur EKS Anywhere, consultez la documentation EKS Anywhere.

Parcourez les produits conteneurisés à l'aide de la console Amazon ECS

Vous pouvez également rechercher des produits de conteneur dans la console Amazon ECS. Le volet de navigation contient des liens permettant de découvrir de nouveaux produits AWS Marketplace et de consulter les abonnements existants.

Résilier un abonnement

Pour résilier un abonnement à un produit, utilisez la page Vos logiciels.

Produits en conteneur avec prix contractuel

Certains vendeurs proposent des produits logiciels basés sur des conteneurs publics avec un modèle de tarification contractuelle, dans lequel vous acceptez d'effectuer un paiement initial unique pour des quantités discrètes de licences permettant d'accéder au produit logiciel pendant une durée de votre choix, facturées à l'avance par le biais de votre. Compte AWS

Example de l'achat de différents types de licences en différentes quantités

Par exemple, vous pouvez acheter 10 licences d'accès utilisateur et 5 licences administratives pour un an. Vous pouvez choisir de renouveler automatiquement les licences.

En outre, certaines entreprises proposent des produits logiciels privés basés sur des conteneurs avec un modèle de tarification contractuelle. Une offre privée a généralement une durée fixe que vous ne pouvez pas modifier.

Vous pouvez acheter un contrat de produit logiciel basé sur un conteneur en utilisant la page détaillée du produit sur. AWS Marketplace Si cette option est disponible, l'AMI avec les prix contractuels apparaît pour le mode de livraison sur la page détaillée du produit. Lorsque vous effectuez l'achat, vous serez dirigé vers le site Web du produit pour la configuration et la configuration du compte. Les frais d'utilisation apparaîtront alors sur votre rapport Compte AWS de facturation habituel.

Abonnement à un produit en conteneur avec offre publique de prix contractuels en AWS Marketplace

Pour souscrire à une offre publique, un produit basé sur un conteneur avec un modèle de tarification contractuelle

> **Note**
>
> Pour plus d'informations sur l'abonnement à l'aide d'Amazon EKS, consultez la section Gestion des modules complémentaires Amazon EKS.

1. Connectez-vous AWS Marketplace et trouvez un produit logiciel basé sur des conteneurs avec un modèle de tarification contractuelle.

2. Sur la page Achats, consultez les informations tarifaires.

   Vous pouvez consulter les unités et le taux par rapport à chaque durée (en mois).

3. Pour démarrer l'abonnement, choisissez Continuer à vous abonner.

   Pour enregistrer ce produit sans vous abonner, choisissez Enregistrer dans la liste.

4. Créez un accord en consultant les informations de tarification et en configurant les conditions du produit logiciel.

   a. Choisissez la durée du contrat : 1 mois, 12 mois, 24 mois ou 36 mois.

   b. Sous Paramètres de renouvellement, choisissez si vous souhaitez renouveler automatiquement le contrat.

   c. Sous Options de contrat, choisissez une quantité pour chaque unité.

   Le prix total du contrat est affiché sous Détails des prix.

5. Après avoir effectué vos sélections, choisissez Créer un contrat.

Le prix total du contrat vous est facturé Compte AWS et une licence est générée dansAWS License Manager.

> **Note**
>
> Le traitement de l'abonnement et la génération d'une licence dans votre compte License Manager pour le produit logiciel peuvent prendre jusqu'à 10 minutes.

Abonnement à un produit en conteneur avec offre privée de prix contractuel en AWS Marketplace

Pour souscrire à une offre privée, un produit basé sur un conteneur avec un modèle de tarification contractuelle

> **Note**
>
> Pour plus d'informations sur l'abonnement à l'aide d'Amazon EKS, consultez la section Gestion des modules complémentaires Amazon EKS.

1. Connectez-vous AWS Marketplace à votre compte acheteur.
2. Consultez l'offre privée.
3. Sur la page Achats, consultez les informations tarifaires.

   Vous pouvez voir les unités et le taux pour chaque durée (en mois).
4. Choisissez Continuer à vous abonner pour démarrer l'abonnement.
5. Créez un accord en consultant les informations de tarification et en configurant les conditions du produit logiciel.

   La durée du contrat est déjà fixée par le vendeur et ne peut pas être modifiée.
6. Sous Options de contrat, choisissez une quantité pour chaque unité.
7. Consultez le prix total du contrat sous Détails des prix.

   Vous pouvez également consulter l'offre publique en choisissant Afficher l'offre sous Autres offres disponibles.
8. Après avoir effectué vos sélections, choisissez Créer un contrat.

> **Note**
>
> Le traitement de l'abonnement et la génération d'une licence dans votre compte License Manager pour le produit logiciel peuvent prendre jusqu'à 10 minutes.

Accès au logiciel

Pour accéder au produit logiciel basé sur des conteneurs

1. Sur la AWS Marketplace console, accédez à Afficher l'abonnement et consultez la licence du produit logiciel.
2. Sur la page Achats :

   a. Choisissez Gérer la licence pour consulter, autoriser l'accès et suivre l'utilisation de vos droits dans. AWS License Manager
   b. Choisissez Continue to Configuration (Continuer vers Configuration).
3. Sur la page de lancement, consultez les détails de l'image du conteneur et suivez les instructions fournies.

Lors de la création d'un cluster Amazon Elastic Container Service (Amazon ECS), vous devez ajouter les autorisations (IAM) AWS Identity and Access Management suivantes à votre politique IAM.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
   ]
}
```

Afficher une licence générée

Pour consulter une licence générée

1. Connectez-vous à l'AWS License Manageraide de votreCompte AWS.
2. Sous Licences accordées, consultez toutes les licences que vous avez accordées.
3. Recherchez des licences en saisissant le SKU, le destinataire ou le statut du produit dans la barre de recherche.
4. Choisissez le numéro de licence et consultez les détails de la licence.
5. Vous pouvez consulter l'émetteur (AWS/Marketplace) et les droits (les unités pour lesquelles la licence accorde le droit d'utiliser, d'accéder ou de consommer une application ou une ressource).

Modifier un contrat existant

S'ils ont déjà un engagement initial pour un produit Container, AWS Marketplace les acheteurs peuvent modifier certains aspects du contrat. Un contrat de conteneur est soutenu par des offres basées sur les termes du contrat, par opposition à des offres de prix de consommation flexibles (FCP) horaires ou annuels. Cette fonctionnalité n'est disponible que pour les applications intégrées àAWS License Manager. Les acheteurs peuvent acheter des licences supplémentaires dans le cadre de la même offre prévue dans le contrat en cours. Toutefois, les acheteurs ne peuvent pas réduire le nombre de droits achetés dans le cadre du contrat. Les acheteurs peuvent également annuler le renouvellement automatique de l'abonnement si l'option est activée par le vendeur.

> **Note**
>
> Une offre de contrat avec échéancier de paiement flexible (FPS) ne peut pas être modifiée. Aucune modification des droits n'est disponible pour l'acheteur pour un contrat acheté par FPS. Un droit est le droit d'utiliser, d'accéder ou de consommer une application ou une ressource. Les offres FPS ne sont pas modifiables.

Gérez votre abonnement

1. Sur la AWS Marketplace console, accédez à Afficher l'abonnement et consultez la licence du produit logiciel.
2. Sur la page Achats, sélectionnez Gérer la licence.
3. Dans la liste, sélectionnez Afficher les termes.
4. Dans la section Options du contrat, augmentez vos droits à l'aide des flèches. Vous ne pouvez pas réduire le nombre de droits en dessous du nombre de droits achetés.
5. Les détails du contrat et le prix total s'affichent dans la section Détails des prix.

Pour annuler le renouvellement automatique de votre abonnement

1. Sur la AWS Marketplace console, accédez à Afficher l'abonnement et consultez la licence du produit logiciel.
2. Sur la page Achats, sélectionnez Gérer la licence.
3. Sur la page Abonnement, recherchez la section Paramètres de renouvellement.
4. Assurez-vous de bien comprendre les termes et conditions relatifs à l'annulation.

5. Cochez la case pour annuler l'option de renouvellement automatique.

Lancement d'un logiciel de conteneur depuis AWS Marketplace

Une fois que vous avez un abonnement actif à un produit conteneurAWS Marketplace, l'étape suivante consiste à lancer le logiciel. Pour lancer le logiciel, suivez les instructions incluses dans l'une des options d'expédition fournies par le vendeur. DansAWS Marketplace, une option d'expédition est une procédure facultative proposée par le vendeur pour lancer son produit dans votre environnement. Pour les produits en conteneur, le vendeur peut proposer jusqu'à quatre options d'expédition, qui peuvent utiliser différents modes de livraison et représenter différentes configurations pour le logiciel. Par exemple, un vendeur peut créer une option d'expédition utilisée pour tester le produit et une autre à déployer à grande échelle au sein d'une entreprise.

Vous pouvez voir quelles options d'expédition sont disponibles dans la section Informations d'utilisation de la page détaillée du produit dansAWS Marketplace. Chaque option d'expédition inclut des informations sur les services pris en charge et fournit des informations détaillées sur la version du logiciel. Amazon Elastic Container Service (Amazon ECS) et Amazon Elastic Kubernetes Service (Amazon EKS) sont des exemples de services. Vous pouvez choisir les instructions d'utilisation pour obtenir la documentation du vendeur sur l'utilisation du produit, telle que la connexion à un serveur Web ou la configuration après le lancement.

> **Note**
>
> Pour découvrir comment s'abonner à un produit basé sur un conteneur et le déployer, vous pouvez également consulter les vidéos suivantes :
>
> - Déploiement de AWS Marketplace conteneurs sur des clusters Amazon ECS (3:34)
> - Déploiement de produits AWS Marketplace basés sur des conteneurs à l'aide d'Amazon ECS Anywhere (5:07)

Déploiement de produits basés sur des conteneurs AWS Marketplace à l'aide d'ECS Anywhere

Lancez le logiciel de conteneur depuis AWS Marketplace

Pour lancer un logiciel de conteneur à partir de AWS Marketplace

1. Connectez-vous à AWS Marketplace.

2. Parcourez AWS Marketplace et recherchez le produit contenant le logiciel que vous souhaitez lancer. Vous devez être abonné au produit pour lancer son logiciel. Pour plus d'informations sur la recherche et l'abonnement à des produits en conteneur dansAWS Marketplace, voirRechercher et s'abonner à des produits de conteneur.
3. Choisissez Continuer pour vous abonner sur la page de détails du produit.
4. Choisissez Continue to Configuration (Continuer vers Configuration). Si vous ne voyez pas le bouton, il se peut que vous deviez d'abord accepter les conditions ou que vous n'ayez pas d'abonnement au produit.
5. Dans Option d'expédition, sélectionnez une option d'expédition dans la liste d'options fournie par le vendeur. Après avoir sélectionné une option d'expédition, vous pouvez voir les services que vous pouvez lancer dans Services pris en charge. Pour plus d'informations sur les options d'expédition, consultezOptions d'expédition des produits en conteneur.
6. Choisissez Continuer pour lancer.
7. Suivez les instructions fournies par le vendeur pour lancer le produit. Les instructions sont différentes pour chaque option d'expédition. Pour plus d'informations, consultez Lancement avec une option de traitement des images du conteneur ou Lancement avec une option Helm Fulfillment.
8. Facultatif : choisissez les instructions d'utilisation pour obtenir la documentation du vendeur expliquant comment configurer et utiliser le produit après son lancement.

Options d'expédition des produits en conteneur

Vous pouvez consulter les options d'expédition disponibles dans la section Informations d'utilisation de la page détaillée d'un produit. Outre les options d'expédition proposées par le vendeur, vous trouverez AWS Marketplace des instructions pour extraire les images Docker directement depuis Amazon Elastic Container Registry (Amazon ECR).

Les options d'expédition étant fournies par le vendeur, leurs noms et leur contenu seront différents pour chaque produitAWS Marketplace. Bien que les méthodes soient propres à chaque produit et à chaque vendeur, chaque option d'expédition doit comporter un mode de livraison. Vous pouvez considérer un mode de livraison comme un type d'option d'expédition. Les trois méthodes de livraison disponibles pour les produits en conteneur sont Container image, Helm chart et Add on for Amazon EKS.

Lancement avec une option de traitement des images du conteneur

Pour une option d'expédition avec une méthode de livraison d'images Container, utilisez les instructions fournies par le vendeur pour lancer le produit. Cela se fait en extrayant des images Docker directement depuis Amazon ECR. Les étapes générales du lancement du produit sont les suivantes :

1. Vérifiez que vous avez installé les dernières versions de AWS Command Line Interface (AWS CLI) et Docker. Pour plus d'informations, consultez la section Utilisation d'Amazon ECR AWS CLI dans le guide de l'utilisateur d'Amazon Elastic Container Registry.
2. Authentifiez votre client Docker auprès de votre registre Amazon ECR. La procédure à suivre dépend de votre système d'exploitation.
3. Extrayez toutes les images Docker à l'aide de l'image Amazon ECR Amazon Resource Name (ARN) fournie. Pour plus d'informations, consultez la section Extraction d'une image dans le guide de l'utilisateur d'Amazon Elastic Container Registry.
4. Consultez les instructions d'utilisation ou les liens externes fournis par le vendeur pour obtenir des informations sur l'utilisation du produit.

Lancement avec une option Helm Fulfillment

Pour une option d'expédition avec un mode de livraison Helm, utilisez les instructions fournies par le vendeur pour lancer le produit. Cela se fait en installant un graphique Helm à l'aide de la CLI Helm. Vous pouvez lancer l'application sur un cluster Amazon EKS existant, sur un cluster autogéré sur EKS Anywhere Amazon Elastic Compute Cloud (Amazon EC2) ou sur site.

> **Note**
>
> Votre environnement de lancement doit utiliser la version 3.7.1 de la CLI Helm. Pour une liste des versions de Helm, voir les versions de Helm sur GitHub.

Si le vendeur l'a activé QuickLaunch, vous pouvez l'utiliser pour lancer l'application. QuickLaunch est une fonctionnalité AWS Marketplace qui permet AWS CloudFormation de créer un cluster Amazon EKS et de lancer l'application dessus. Pour plus d'informations sur QuickLaunch, voirQuickLaunch dans AWS Marketplace.

Les instructions sont fournies par le vendeur et sont différentes pour chaque vendeur et chaque produit. Les étapes générales pour lancer un produit avec une option d'expédition Helm sont les suivantes :

Pour lancer un produit avec une option d'expédition Helm

1. Suivez les étapes 1 à 6 et choisissez une option d'expédition avec un mode de livraison basé sur un schéma Helm. Lancez le logiciel de conteneur depuis AWS Marketplace
2. Dans Launch target, choisissez l'environnement dans lequel vous souhaitez effectuer le déploiement :

   - Choisissez Kubernetes géré par Amazon pour déployer l'application dans Amazon EKS. Si le vendeur l'a activé QuickLaunch, vous pouvez l'utiliser pour créer un nouveau cluster Amazon EKS et le lancer dessus.
   - Choisissez Kubernetes autogéré pour déployer l'application dans EKS Anywhereou sur n'importe quel cluster Kubernetes exécuté dans Amazon EC2 ou sur site.
3. En cas de lancement dans un cluster Kubernetes géré par Amazon :

   a. Pour lancer sur un cluster existant dans Amazon EKS, sous Méthode de lancement, choisissez Lancer sur un cluster existant et suivez les instructions de lancement. Les instructions incluent la création d'un rôle AWS Identity and Access Management (IAM) et le lancement de l'application. Vérifiez que vous utilisez la version 3.7.1 de la CLI Helm.

   b. QuickLaunch Pour créer un nouveau cluster Amazon EKS et le lancer dessus, sous Méthode de lancement, choisissez Lancer sur un nouveau cluster EKS avec QuickLaunch. Choisissez Launch pour être redirigé afin de créer une pile dans la AWS CloudFormation console. Cette pile créera un cluster Amazon EKS et déploiera l'application en installant le graphique Helm fourni par le vendeur.

   c. Sur la page Création rapide d'une pile, dans Nom de la pile, saisissez un nom pour cette pile.

   d. Passez en revue les informations de la vignette Paramètres et fournissez toutes les informations nécessaires. Passez en revue et sélectionnez les remerciements dans Fonctionnalités, puis choisissez Create stack.

> **Note**
>
> Pour plus d'informations QuickLaunch, notamment sur les AWS CloudFormation piles et le cluster Amazon EKS créé, consultezQuickLaunch dans AWS Marketplace.

4. En cas de lancement dans un cluster Kubernetes autogéré :

   a. Vérifiez que vous utilisez la version 3.7.1 de la CLI Helm.

   b. Choisissez Create token pour générer un jeton de licence et un rôle IAM. Ce jeton et ce rôle sont utilisés pour communiquer avec les utilisateurs AWS License Manager afin de valider les droits relatifs aux produits.

      > **Note**
      >
      > Le nombre maximum de jetons de licence pour un compte est de 10.

   c. Choisissez Télécharger au format CSV pour télécharger un fichier .csv contenant les informations du jeton généré. Comme pour tous les secrets et mots de passe, stockez le fichier .csv dans un endroit sûr.

   d. Exécutez les commandes dans Enregistrer en tant que secret Kubernetes pour enregistrer le jeton de licence et le rôle IAM en tant que secret dans votre cluster Kubernetes.
   Ce secret est utilisé lorsque vous installez le graphique Helm et lancez l'application.
   AWS Marketplaceutilise le secret pour vérifier l'éligibilité à ce produit.

   e. Exécutez les commandes dans Launch l'application à l'aide d'un jeton pour installer le graphique Helm qui déploie l'application sur votre cluster.

   f. Choisissez les instructions d'utilisation pour obtenir la documentation du vendeur expliquant comment configurer et utiliser le produit après son lancement.

   g. Facultatif : utilisez les commandes fournies dans [Facultatif] Télécharger des artefacts pour télécharger les images des conteneurs du produit et les diagrammes Helm localement.

Lancement avec une option d'expédition Amazon EKS

Pour une option d'exécution avec un module complémentaire pour le mode de livraison Amazon EKS, utilisez la console Amazon EKS pour déployer le logiciel sur votre cluster Amazon EKS. Les étapes générales du lancement du produit sont les suivantes :

Pour lancer un produit avec une option d'expédition Amazon EKS

1. Après avoir souscrit au produit, accédez à la page de configuration et choisissez Continuer vers la console Amazon EKS pour accéder à la console Amazon EKS.
2. Dans la console Amazon EKS, choisissez l'Région AWSendroit où votre cluster est déployé. Sélectionnez le cluster dans lequel vous souhaitez déployer votre logiciel.
3. Choisissez l'onglet Modules complémentaires.
4. Choisissez Obtenir d'autres modules complémentaires, faites défiler l'écran pour trouver le module complémentaire que vous souhaitez déployer, puis cliquez sur Suivant.
5. Sélectionnez la version que vous souhaitez déployer, puis cliquez sur Next. Pour plus d'informations sur le déploiement d'Amazon EKS, consultez les modules complémentaires EKS.
6. Passez en revue vos sélections et choisissez Créer.

QuickLaunch dans AWS Marketplace

Si le vendeur a QuickLaunch activé une option d'expédition, vous pouvez l'utiliser pour créer un cluster Amazon EKS et y déployer une application de conteneur. Avec QuickLaunch, vous pourrez AWS CloudFormation configurer et créer un cluster Amazon EKS et y lancer une application conteneur. Avec QuickLaunch, vous pouvez lancer une application conteneur à des fins de test. Pour l'utiliser QuickLaunch, suivez les étapes décrites dansLancement avec une option Helm Fulfillment.

Pour créer un cluster Amazon EKS sur lequel l'application peut être déployée, créez une CloudFormation pile. Une pile est un ensemble de ressources AWS que vous gérez comme une seule unité. Toutes les ressources d'une pile sont définies par son modèle CloudFormation . Dans QuickLaunch, les ressources de la pile incluent les informations requises pour créer le cluster Amazon EKS et lancer l'application. Pour plus d'informations sur les pilesAWS CloudFormation, consultez la section Utilisation des piles dans le Guide de l'AWS CloudFormationutilisateur.

Une fois le cluster créé, QuickLaunch lance l'application sur celui-ci en installant le graphique Helm fourni par le vendeur sur le cluster. QuickLaunch gère cela pour vous dans le cadre de la création de la pile qui crée également le cluster Amazon EKS.

Produits de Machine Learning

AWS Marketplace contient une catégorie de produits pour l'apprentissage automatique auxquels vous pouvez vous abonner à travers AWS Marketplace. La catégorie de produits est Apprentissage

automatique. Les produits de cette catégorie incluent des packages de modèles et des algorithmes d'apprentissage automatique (ML).

Vous pouvez parcourir et rechercher des centaines de packages de modèles et d'algorithmes ML dans un large éventail de sous-catégories, telles que la vision par ordinateur, le traitement du langage naturel, la reconnaissance vocale, le texte, les données, la voix, l'image, l'analyse vidéo, la détection des fraudes et l'analyse prédictive.

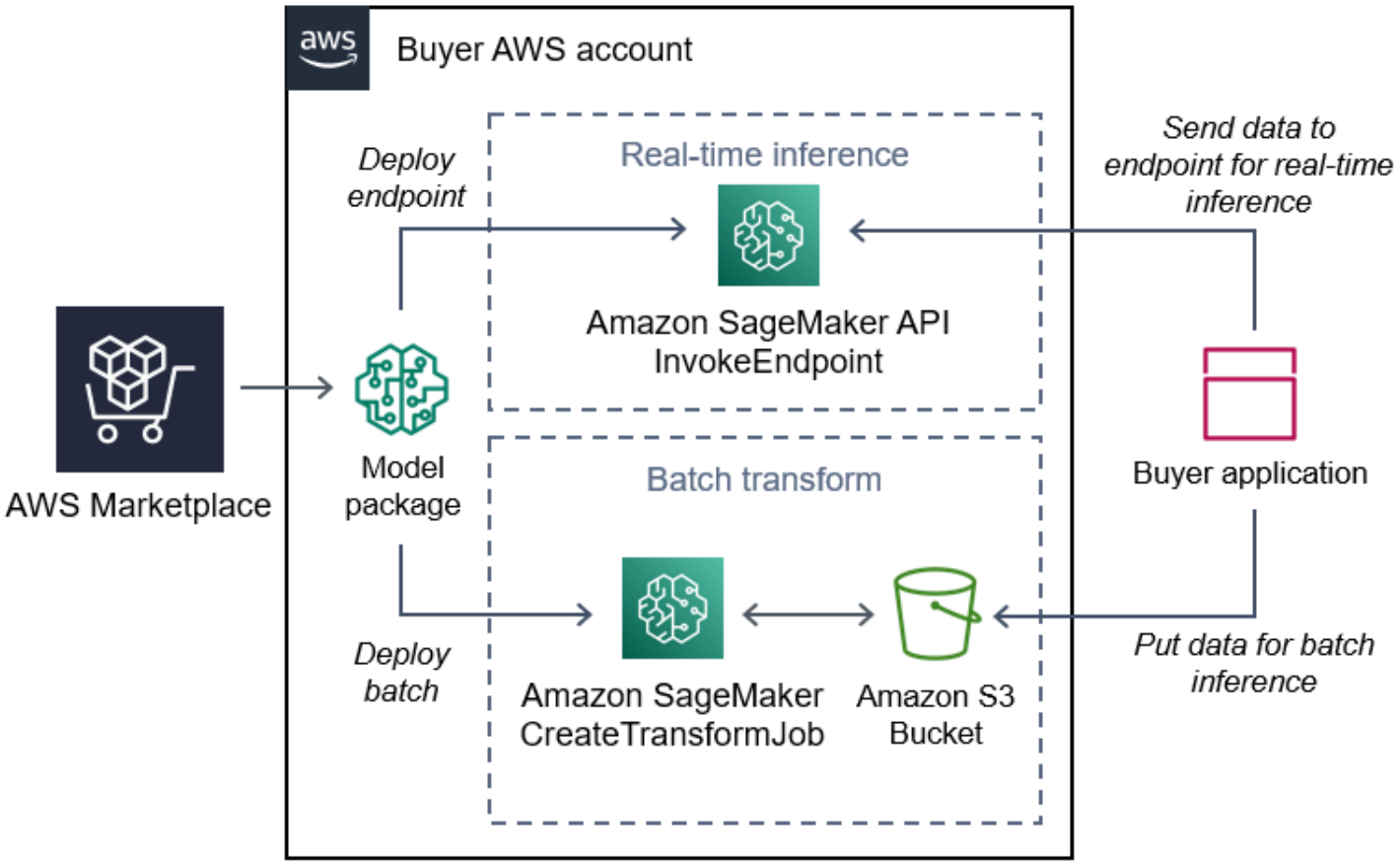
Pour évaluer la qualité et la pertinence d'un modèle, vous pouvez consulter les descriptions de produit, les instructions d'utilisation, les avis des clients, des exemples de bloc-notes Jupyter, la tarification et les informations de support. Vous déployez des modèles directement depuis la SageMaker console Amazon, via un bloc-notes Jupyter, avec le SageMaker SDK Amazon ou à l'aide du. AWS Command Line Interface AWS CLI Amazon SageMaker fournit un environnement sécurisé pour exécuter vos tâches de formation et d'inférence en effectuant une analyse statique de tous les produits Marketplace.

Package SageMaker modèle Amazon

Un package de SageMaker modèle Amazon est un modèle de machine learning préentraîné unique identifié par un Amazon Resource Name (ARN) sur Amazon SageMaker. Les clients utilisent un package modèle pour créer un modèle sur Amazon SageMaker. Le modèle peut ensuite être utilisé avec des services d'hébergement pour exécuter une inférence en temps réel ou avec une transformation par lots pour exécuter une inférence par lots dans Amazon. SageMaker

Le schéma suivant montre le flux de travail pour l'utilisation de modèles de produits d'emballage.

1. LeAWS Marketplace, vous trouvez un modèle de produit et vous y abonnez.
2. Vous déployez le composant d'inférence du produit SageMaker pour effectuer une inférence (ou une prédiction) en temps réel ou par lots.



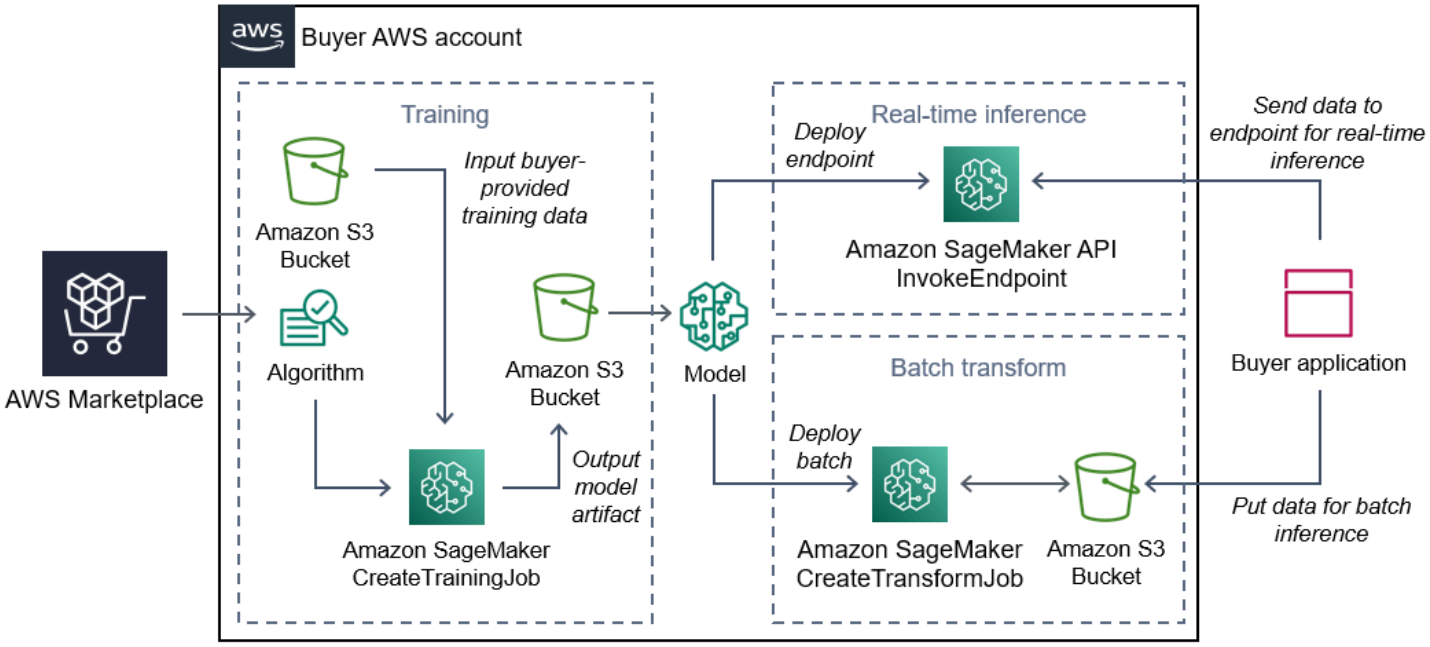
SageMaker Algorithme Amazon

Un SageMaker algorithme Amazon est une SageMaker entité Amazon unique identifiée par un ARN. Il comprend deux composants logiques : la formation et l'inférence.

Le schéma suivant montre le flux de travail d'utilisation des produits algorithmiques.

1. LeAWS Marketplace, vous trouvez un produit algorithmique et vous vous y abonnez.
2. Vous utilisez le composant formation du produit pour créer une tâche de formation ou une tâche de réglage à l'aide de votre jeu de données d'entrée dans Amazon SageMaker pour créer des modèles d'apprentissage automatique.
3. Lorsque le composant de formation du produit est terminé, il génère les artefacts du modèle d'apprentissage automatique.
4. SageMaker enregistre les artefacts du modèle dans votre compartiment Amazon Simple Storage Service (Amazon S3).

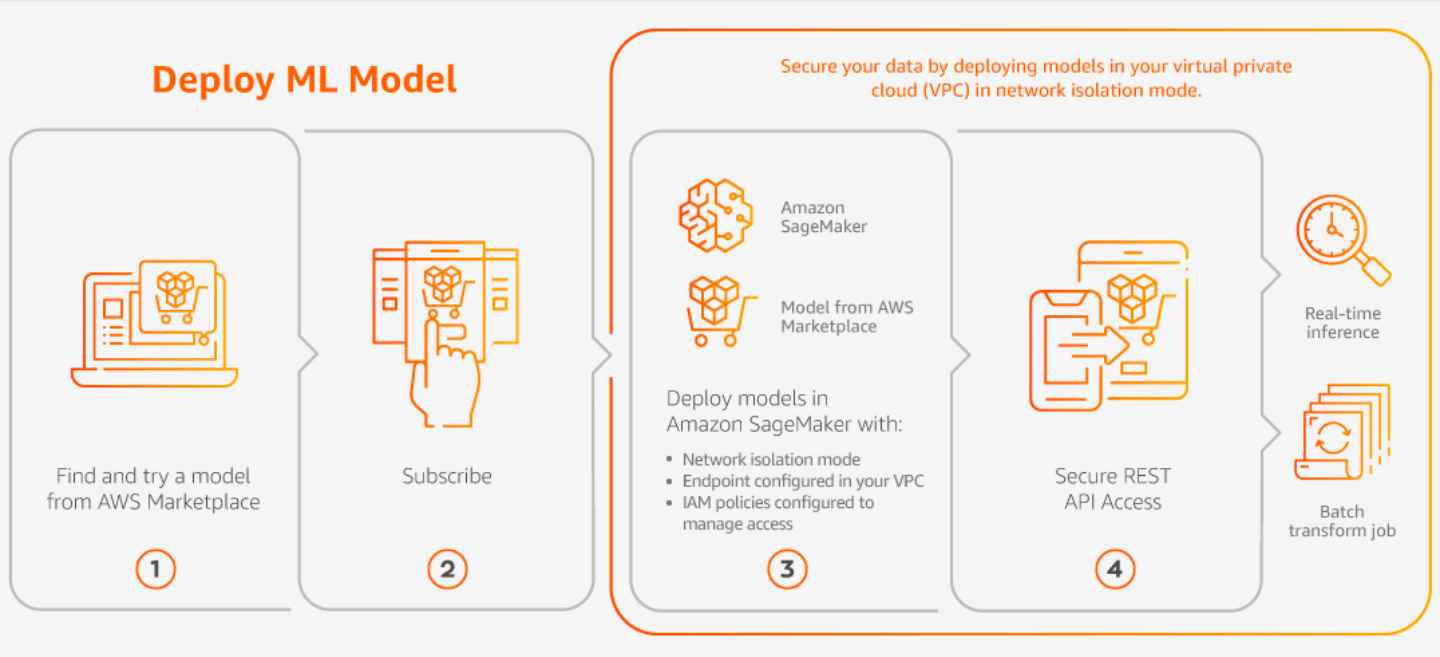
5. Dans SageMaker, vous pouvez ensuite déployer le composant d'inférence du produit à l'aide des artefacts de modèle générés pour effectuer une inférence (ou une prédiction) en temps réel ou par lots.



Rechercher, s'abonner et déployer

Le schéma suivant présente un aperçu du processus de recherche, d'abonnement et de déploiement d'un produit de machine learning sur Amazon SageMaker.

1. Trouvez et essayez un modèle de AWS Marketplace
2. Abonnez-vous au produit ML
3. Déployer des modèles dans Amazon SageMaker
4. Utilisez des API REST sécurisées
5. Exécuter
   - Inférence en temps réel
   - Tâche de transformation par lots



Vous ne payez que pour votre utilisation, sans frais minimaux ni engagements initiaux. AWS Marketplacefournit une facture consolidée pour les algorithmes et les packages de modèles, ainsi que les frais d'utilisation de l'AWSinfrastructure.

Les sections suivantes expliquent comment trouver un produit ML, s'y abonner et le déployer.

Rubriques

- Trouver un produit d'apprentissage automatique
- Abonnement à un produit d'apprentissage automatique
- Déploiement d'un produit de machine learning

Trouver un produit d'apprentissage automatique

Pour trouver des SageMaker modèles, des packages et des algorithmes Amazon

1. Connectez-vous au site Web AWS Marketplace.
2. Sous Trouvez les AWS Marketplace produits qui répondent à vos besoins, utilisez le menu déroulant Catégories pour trouver la sous-catégorie Machine Learning qui vous intéresse.
3. Vous pouvez affiner votre recherche en appliquant les filtres de type de ressource, catégorie et prix.
4. À partir des résultats de recherche, accédez à la page détaillée du produit.

5. Consultez la description du produit, les instructions d'utilisation, les avis des clients, les exigences en matière de données, les exemples de blocs-notes Jupyter, ainsi que les informations sur les prix et le support.

Abonnement à un produit d'apprentissage automatique

Pour vous abonner aux packages SageMaker modèles et aux algorithmes Amazon

1. Sur la page détaillée du produit, choisissez Continuer pour vous abonner.
2. Sur la page d'approvisionnement, consultez les informations sur les prix des produits et le contrat de licence utilisateur final (EULA).
3. Choisissez Continuer pour vous abonner.

Déploiement d'un produit de machine learning

Pour déployer des packages de SageMaker modèles et des algorithmes Amazon

1. Vérifiez que vous disposez d'un abonnement valide à l'algorithme ou au package modèle en accédant à Your Marketplace Software.
2. Configurez le produit (par exemple, en sélectionnant une version ou une région de déploiement spécifique) sur le AWS Marketplace site Web.

   Une fois que vous vous êtes abonné à un package modèle ou à un produit algorithmique, celui-ci est ajouté à votre liste de produits dans la SageMaker console. Vous pouvez également utiliser AWS les SDK, le AWS Command Line Interface (AWS CLI) ou la SageMaker console pour créer un point de terminaison d'inférence REST entièrement géré ou effectuer une inférence sur des lots de données.
3. Consultez la page détaillée SageMaker du produit Amazon en choisissant Afficher sur Amazon SageMaker.
4. Depuis la SageMaker console Amazon, vous pouvez déployer les packages de modèles et les algorithmes à l'aide de la SageMaker console Amazon, du bloc-notes Jupyter, des commandes Amazon SageMaker CLI ou des opérations d'API.

Pour plus d'informations sur le déploiement sur Amazon SageMaker, consultez Getting Started.

Produits de services professionnels

AWS Marketplaceinclut des produits qui sont des services professionnels deAWS Marketplacevendeurs. Vous pouvez trouver ces produits dans laServices professionnelscatégorie lors de la recherche dansAWS Marketplace. Vous vous abonnez et vous achetez ces produits viaAWS Marketplace, mais vous travaillerez avec le vendeur pour mettre en place les services professionnels qui répondent à vos besoins.

Achat de services professionnels

Vous pouvez rechercher des services professionnels en utilisant leServices professionnelsCatégorie dansAWS Marketplace. Lorsque vous trouvez un produit qui vous intéresse, demandez une offre au vendeur. Étant donné que les services professionnels impliquent généralement une collaboration, vous devez fournir certaines informations supplémentaires au vendeur afin de finaliser l'achat. Vous pouvez également profiter de cette occasion pour négocier les prix et tout autre détail du service qui doit être résolu. Vous recevrez une offre privée pour le produit. Pour plus d'informations sur les offres privées, consultez.Offres privées.

Pour acheter un produit de services professionnels

1. Accéder àAWS Marketplaceet connectez-vous à votreAWS, puis recherchez et recherchez le produit de services professionnels que vous souhaitez acheter.
2. Sur la page des détails du produit, sélectionnezContinuer.
3. Dans la pageDemande de service, ajoutez les informations supplémentaires nécessaires au vendeur pour créer l'offre, y compris votre nom, votre adresse e-mail, le nom de votre société et toute autre information pouvant être utile au vendeur, notamment les besoins commerciaux, les délais et les exigences du contrat.
4. Le vendeur vous contactera via l'adresse e-mail que vous avez fournie pour définir les détails de votre offre. Une fois que vous aurez accepté, le vendeur vous enverra un lien vers l'offre dansAWS Marketplace. Ouvrez le lien dans un navigateur et connectez-vous à votreAWS.
5. Consultez les détails de l'offre sur la page d'achat que vous avez ouverte auprès du vendeur. Assurez-vous que l'offre correspond au service que vous attendez et au prix que vous attendez. Vérifiez également les conditions, que vous payiez une somme forfaitaire ou une série de frais. Si l'offre est correcte, continuez. Dans le cas contraire, contactez le vendeur pour apporter des modifications.

6. UnderConfiguration du contrat, choisissez la configuration que vous souhaitez utiliser pour votre contrat. Par exemple, si vous souscrivez un contrat de support, il peut y avoir des options pourArgent,Gold, ouPlatinecontrats, avec des prix différents.
7. Tâche de sélectionCREATE CONTRACTpour acheter le service. Le vendeur doit vous contacter dans les 2 jours ouvrables pour vous fournir les instructions d'utilisation du service.

Produits SaaS

Pour les produits SaaS (Software as a Service), vous vous abonnez aux produits par le biais de l'environnement du vendeur de logicielsAWS Marketplace, mais vous accédez au produit dans l'environnement du vendeur de logiciels.

Rubriques

Modèles de tarification

AWS Marketplacepropose les modèles de tarification suivants.

Abonnements SaaS basés sur l'utilisation

Avec les abonnements SaaS basés sur l'utilisation, le vendeur du logiciel suit votre utilisation et vous ne payez que pour ce que vous utilisez. Ce modèle de pay-as-you-go tarification est similaire à celui de nombreux autresServices AWS. La facturation en fonction de votre utilisation d'un produit SaaS est gérée par le biais de votre facture AWS.

Pour vous abonner à l'aide de l'abonnement SaaS basé sur l'utilisation

1. Sur la page détaillée du produit, choisissez Afficher les options d'achat pour démarrer le processus d'abonnement.
2. Vérifiez l'abonnement, puis choisissez S'abonner sur la page d'abonnement.

> **Note**
>
> Certains produits proposent une option de déploiement Quick Launch, qui réduit le temps et les ressources nécessaires à la configuration, au déploiement et au lancement

des logiciels. Ces produits sont identifiés à l'aide d'un badge Quick Launch. Pour plus d'informations, consultez the section called “Lancement rapide”.

Engagements initiaux en matière de SaaS

Certaines entreprises proposent des contrats SaaS à l'achat dès le départ. AWS Marketplace Cette option vous permet d'acheter des quantités discrètes de licences ou d'ingérer des données pour ces produits. Ensuite, vous pouvez facturer ces produits, à l'avance, par le biais de votreCompte AWS. Par exemple, vous pouvez acheter 10 licences d'accès utilisateur pour une année, ou vous acheter la collecte de 10 Go de données par jour pendant un an.

Lorsque vous effectuez l'achat, vous êtes dirigé vers le site Web du produit pour configurer votre compte, sauf si le lancement rapide est activé. Les frais d'utilisation apparaissent ensuite sur votre rapport Compte AWS de facturation habituel.

> **Note**
>
> Pour plus d'informations sur l'expérience de lancement rapide, consultezthe section called “Lancement rapide”.

Pour s'abonner avec un contrat SaaS

1. Sur la page détaillée du produit, choisissez Afficher les options d'achat pour démarrer le processus d'abonnement. Vous pouvez choisir les quantités ou unités souhaitées, la durée de l'abonnement (si plusieurs options sont disponibles) et le renouvellement automatique.
2. Une fois que vous avez effectué vos sélections, cliquez sur Create Contract (Créer contrat).
3. Choisissez Set Up Your Account (Configuration de votre compte), pour être dirigé vers le site Web de l'entreprise. Pendant que votre compte est configuré et que le paiement est en cours de vérification, vous verrez que votre contrat est en attente sur la page de description AWS Marketplace du produit.

> **Note**
>
> Certains produits proposent une option de déploiement Quick Launch, qui réduit le temps et les ressources nécessaires à la configuration, au déploiement et au lancement

des logiciels. Ces produits sont identifiés à l'aide d'un badge Quick Launch. Pour plus d'informations, consultez the section called “Lancement rapide”.

Une fois la configuration terminée, un lien permettant de configurer votre compte est disponible sur la page du produit. Le logiciel apparaît sous Your Marketplace Software lorsque vous êtes connecté à votre AWS Marketplace compte. Maintenant, vous pouvez commencer à utiliser le logiciel. Si vous n'avez pas terminé le processus de configuration de votre compte, vous êtes invité à le faire lorsque vous revenez sur AWS Marketplace ce produit.

Accédez à l'abonnement logiciel depuis le site Web de l'éditeur de logiciels en utilisant le compte que vous avez créé sur son site Web. Vous pouvez également trouver des liens vers des sites Web pour les abonnements logiciels que vous AWS Marketplace avez achetés dans Your Marketplace Software lorsque vous êtes connecté à votre AWS Marketplace compte.

Essais gratuits de SaaS

Certains fournisseurs proposent des essais gratuits pour leurs produits SaaS à AWS Marketplace des fins d'évaluation. Vous pouvez effectuer une recherche dans les produits SaaS AWS Marketplace et filtrer les résultats pour n'afficher que ceux dont les versions d'essai sont gratuites. Les résultats de recherche indiquent quels produits proposent des essais gratuits. Tous les produits d'essai gratuit affichent le badge d'essai gratuit à côté du logo du produit. Sur la page d'achat du produit, vous pouvez trouver la durée de la période d'essai gratuit et la quantité d'utilisation du logiciel libre incluse dans l'essai.

Pendant l'essai gratuit ou après son expiration, vous pouvez prendre une décision d'achat en négociant une offre privée ou en souscrivant à une offre publique. Les essais gratuits du SaaS ne seront pas automatiquement convertis en contrats payants. Si vous ne souhaitez plus bénéficier de l'essai gratuit, vous pouvez le laisser expirer.

Vous pouvez consulter vos abonnements en sélectionnant Gérer les abonnements dans la AWS Marketplace console.

> **Note**
>
> Chacun d'entre eux n'Compte AWSest éligible qu'à un seul essai gratuit par produit.

Souscrire à un contrat SaaS (offre d'essai gratuite)

Pour souscrire à un contrat SaaS (offre d'essai gratuite)

1. Connectez-vous à la AWS Marketplace console, puis choisissez Découvrir les produits AWS Marketplace dans le menu.
2. Dans le panneau Affiner les résultats, accédez à Essai gratuit, puis sélectionnez Essai gratuit.
3. Pour les modes de livraison, sélectionnez SaaS.
4. Pour le modèle de tarification, sélectionnez Engagement initial pour voir tous les produits proposant des essais gratuits. Tous les produits éligibles sont dotés d'un badge d'essai gratuit.
5. Sélectionnez le produit SaaS que vous souhaitez.
6. Choisissez Essayer gratuitement sur la page détaillée du produit.
7. Pour le type d'offre, sélectionnez une option d'essai gratuit.
8. Pour Acheter, choisissez Créer un contrat, puis Accepter le contrat.
9. Choisissez Configurer votre compte pour terminer votre inscription et commencer à utiliser votre logiciel.

Souscrire à une offre d'essai gratuite par abonnement SaaS

Pour souscrire à une offre d'essai gratuite d'abonnement SaaS

1. Connectez-vous à la AWS Marketplace console, puis choisissez Découvrir les produits AWS Marketplace dans le menu.
2. Dans le panneau Affiner les résultats, accédez à Essai gratuit, puis sélectionnez Essai gratuit.
3. Pour les modes de livraison, sélectionnez SaaS.
4. Pour le modèle de tarification, sélectionnez Basé sur l'utilisation pour voir tous les produits proposant des essais gratuits. Tous les produits éligibles sont dotés d'un badge d'essai gratuit.
5. Sélectionnez le produit SaaS que vous souhaitez.
6. Choisissez Essayer gratuitement sur la page détaillée du produit.
7. Pour le type d'offre, sélectionnez une option d'essai gratuit.
8. Pour Acheter, choisissez S'abonner.

Lancement rapide

Quick Launch est une option de AWS Marketplace déploiement disponible pour les produits SaaS sur lesquels Quick Launch est activé. Cela réduit le temps, les ressources et les étapes nécessaires à la configuration, au déploiement et au lancement de votre logiciel. Pour les produits dotés de cette fonctionnalité, vous pouvez choisir d'utiliser le lancement rapide ou de configurer manuellement vos ressources.

Pour rechercher, s'abonner et lancer un produit SaaS à l'aide de l'expérience Quick Launch

1. Accédez à la page AWS Marketplace de recherche.
2. Parcourez AWS Marketplace et recherchez le produit qui contient le logiciel que vous souhaitez lancer. Les produits proposant l'expérience Quick Launch sont dotés d'un badge Quick Launch dans leur description.

   > **Tip**
   >
   > Pour rechercher des produits pour lesquels l'expérience Quick Launch est activée, utilisez le SaaS et les filtres de CloudFormation modèles dans le volet Affiner les résultats.

3. Après vous être abonné au produit, accédez à la page de configuration et de lancement en cliquant sur le bouton Configurer votre compte.
4. Sur la page de configuration et de lancement de l'étape 1 : assurez-vous que vous disposez AWS des autorisations requises, assurez-vous que vous disposez des autorisations nécessaires pour utiliser l'expérience de lancement rapide. Contactez votre AWS administrateur pour demander les autorisations.

   Pour utiliser l'expérience Quick Launch complète, vous devez disposer des autorisations suivantes :

   - `CreateServiceLinkedRole`— Permet AWS Marketplace de créer le rôle `AWSServiceRoleForMarketplaceDeployment` lié au service. Ce rôle lié au service permet AWS Marketplace de gérer les paramètres liés au déploiement, qui sont stockés en tant que secrets dansAWS Secrets Manager, en votre nom.
   - `DescribeSecrets`— Permet d'AWS Marketplaceobtenir des informations sur les paramètres de déploiement transmis par les vendeurs.

- `GetRole`— Permet AWS Marketplace de déterminer si le rôle lié au service a été créé dans le compte.
- `ListSecrets`— Permet AWS Marketplace d'obtenir l'état des paramètres de déploiement.
- `ListRegions`— Permet d'AWS Marketplaceobtenir Régions AWS que l'on ait opté pour le compte courant.
- `ReplicateSecrets`— Permet AWS Marketplace de démarrer la réplication des secrets dans la région sélectionnée dans laquelle vous allez déployer le logiciel.

5. Pour l'étape 2 : connectez-vous à un compte fournisseur existant ou nouveau, cliquez sur le bouton Se connecter ou créer un compte. Le site du vendeur s'ouvre dans un nouvel onglet, dans lequel vous pouvez vous connecter ou créer un nouveau compte. Lorsque vous avez terminé, retournez à la page de configuration et de lancement.
6. Pour l'étape 3 : Configuration du logiciel et de AWS l'intégration, choisissez la manière dont vous souhaitez configurer le produit :

   - AWS CloudFormation— Cliquez sur le bouton Lancer le modèle pour déployer un CloudFormation modèle prédéfini afin de configurer votre produit. CloudFormation À utiliser pour vérifier les paramètres du modèle et compléter les champs obligatoires supplémentaires. Lorsque vous avez terminé, retournez à la page de configuration et de lancement pour lancer votre logiciel.
   - Manuel — Utilisez les instructions fournies par le vendeur pour configurer votre logiciel.
7. Pour l'étape 4 : Lancez votre logiciel, cliquez sur le bouton Lancer le logiciel pour lancer le logiciel.

Produits de données

Vous pouvez utiliserAWS Marketplacepour trouver des produits de données disponibles et vous y abonner via AWS Data Exchange. Pour de plus amples informations, veuillez consulterAbonnement aux produits de données dans AWS Data Exchangedans leGuide de l'utilisateur AWS Data Exchange.

Payer pour des produits

Au début du mois, vous recevez une facture d'Amazon Web Services (AWS) pour vos AWS Marketplace frais. Pour les produits logiciels, la facture inclut un calcul des frais horaires pour le logiciel multipliés par le nombre d'heures d'exécution d'une instance AMI avec ce logiciel. Vous recevez également une facture pour l'utilisation de services d'AWSinfrastructure tels qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) et pour la bande passante.

Si vous êtes Compte AWS basé en Europe, au Moyen-Orient et en Afrique (EMEA), à l'exception de la Turquie et de l'Afrique du Sud, et que votre achat provient d'un vendeur éligible à la zone EMEA, vous recevez une facture d'Amazon Web Services EMEA SARL (). AWS Europe Sinon, vous recevez une facture de AWS Inc.

> **Note**
>
> Pour les achats sous contrat, les frais d'abonnement sont facturés au moment de l'abonnement, plutôt que dans la facture mensuelle consolidée. Les paiements flexibles sur les contrats sont facturés au moment du paiement prévu. Pour les contrats qui comportent des composants d'utilisation (tels qu'un pay-as-you-go modèle), l'utilisation apparaît dans votre facture mensuelle consolidée.

AWS Marketplaceles produits utilisant des topologies complexes peuvent entraîner des frais pour les clusters d'AMI et les autres services d'AWSinfrastructure lancés par le modèle forniAWS CloudFormation.

Par exemple, supposons que vous exécutez un logiciel pendant 720 heures sur une instance de type EC2 small. Les frais du vendeur pour l'utilisation du logiciel sont de 0,12$ par heure et les frais EC2 sont de 0,085$ par heure. À la fin du mois, vous êtes facturé 147,60 USD.

Pour plus d'informations sur l'abonnement à des produits de données, consultez la section Abonnement à des produits de données sur AWS Data Exchange dans le Guide de l'utilisateur d'AWS Data Exchange.

Pour plus d'informations sur le paiement de votre AWS facture, consultez le Guide de AWS Billing l'utilisateur.

Pour plus d'informations sur la gestion de vos paiements dans Amazon Web Services EMEA SARL (AWSEurope), consultez la section Gestion de vos paiements AWSEurope dans le Guide de l'AWS Billingutilisateur.

Rubriques

Bons de commande

Lorsque vous utilisez des bons de commande dans AWS Marketplace et la AWS Billing console, vous recevez des factures AWS qui incluent le numéro de bon de commande défini par le client. Cette approche simplifie le traitement des paiements et la répartition des coûts. DansAWS Marketplace, out-of-cycle les factures incluent les achats qui sont facturés soit immédiatement, soit selon un paiement défini prévu dans une offre privée. En général, pay-as-you-go les frais apparaissent sur une facture d'utilisation AWS Marketplace mensuelle consolidée.

Utilisation des bons de commande pour les AWS Marketplace transactions

Vous pouvez ajouter un bon de commande au moment de la transaction, qui s'appliquera à toutes les out-of-cycle factures suivantes liées à cette transaction.

Les produits suivants prennent en charge les bons de commande :

- Contrats de logiciel en tant que service (SaaS)
- Produits de service professionnels
- Produits pour serveurs (y compris les instances AMI, les conteneurs, les AWS CloudFormation modèles et les diagrammes Helm) avec un modèle de tarification annuel ou contractuel

> **Note**
>
> L'assistance aux bons de commande pour le modèle de tarification annuel n'est disponible que pour les offres privées avec un calendrier de paiement flexible.

Les bons de commande pour le modèle de tarification annuel ne sont pris en charge que pour les offres privées avec un calendrier de paiement flexible. Le bon de commande que vous spécifiez ne s'applique pas aux factures AWS Marketplace mensuelles consolidées relatives aux pay-as-you-go frais.

> **Note**
>
> Pour utiliser les bons de commande dansAWS Marketplace, le compte de gestion de votre AWS organisation doit activer l'AWS Billingintégration. Cette tâche de configuration unique crée un rôle lié à un service, qui permet aux comptes de votre organisation autorisés à s'abonner pour utiliser des bons de commande. Si vous n'activez pas l'intégration, les comptes de votre organisation ne peuvent pas ajouter de bon de commande lors de l'approvisionnement. Pour plus d'informations sur l'intégration, consultez la section Création d'un rôle lié à un service pour. AWS Marketplace

Pour spécifier un bon de commande dans AWS Marketplace

1. Recherchez et préparez-vous à acheter un produit pris en charge auprès deAWS Marketplace.
2. Au cours du processus d'achat, sur la page Configurer votre abonnement logiciel (pour le SaaS), pour Bon de commande, choisissez Ajouter un numéro de bon de commande.
3. Entrez votre numéro de bon de commande dans le champ Numéro de bon de commande.

   Le numéro de votre bon de commande est le numéro ou le texte que vous utilisez pour suivre votre bon de commande dans votre système. Il est généralement émis par un système ou un processus interne. Il peut contenir jusqu'à 200 caractères.

Pour plus de détails sur un bon de commande, y compris les bons de commande fournis lors AWS Marketplace des transactions, utilisez le tableau de bord des bons de commande de la AWS Billing console.

Utilisation de bons de commande à usage général

Pour séparer les AWS Marketplace frais des autres bons de commande, vous pouvez créer un bon de commande avec AWS Marketplace une ligne d'utilisation globale dans la AWS Billing console. AWS Marketplaceles transactions de facturation incluront le bon de commande d'utilisation globale que vous spécifiez si certains critères et paramètres correspondent (par exemple, les entités de facturation). Les out-of-cycle factures qui ont spécifié une AWS Marketplace transaction, un bon de commande constituent une exception. Pour plus d'informations, consultez la section Gestion de vos bons de commande dans le Guide de l'utilisateur d'AWS Billing and Cost Management.

Résolution des problèmes de bons de commande

Les informations du tableau suivant peuvent vous aider à résoudre les problèmes liés aux bons de commande ou à comprendre ce qui se passe dans différents scénarios.

Scénario	Détails
Autorisations insuffisantes	La note s'affiche à côté du champ de saisie du bon de commande si vous n'êtes pas `aws-marketplace:Subscribe` autorisé à vous abonner. Le compte de gestion doit également activer l'AWS Billingintégration. Pour plus d'informations sur l'activation de l'intégration, consultez la section Création d'un rôle lié à un service pour. AWS Marketplace
Le bon de commande n'existe pas	AWS Marketplacecrée un nouveau bon de commande pour vous. Le nouveau bon de commande contient des informations par défaut, sans aucune information de contact.
Notifications de bon de commande manquantes	Les bons de commande sans coordonné es (y compris les bons de commande créés parAWS Marketplace) ne reçoivent pas de notifications par e-mail. Vous pouvez ajouter des informations de contact à un bon de commande dans le tableau de bord des bons

Scénario	Détails
	de commande de la console de facturation et de gestion des coûts.
Numéro de bon de commande incorrect ajouté	Si vous avez saisi un numéro de bon de commande incorrect et que vous devez le mettre à jour, contactez-nous AWS Support pour mettre à jour le numéro de bon de commande.
Le compte d'abonnement est transféré vers une autre organisation	Pour que les bons de commande fonctionnent dans la nouvelle organisation, l'intégration doit être terminée dans la nouvelle organisation. Si l'intégration est terminée et que le support des bons de commande fonctionne dans la nouvelle organisation, lorsque le compte abonné change d'organisation, les nouvelles factures indiquent le numéro du bon de commande dans la nouvelle organisation (et un nouveau bon de commande est créé, si nécessaire).
L'option de bon de commande n'est pas disponible lors du paiement	L'AWS Billingintégration est uniquement disponible pour les contrats SaaS, les produits de service professionnels et les produits de serveur avec une tarification contractuelle, ainsi que pour les produits de serveur avec une tarification annuelle pour les offres privées avec un calendrier de paiement flexible.

Scénario	Détails
Contrats avec pay-as-you-go	La facture du contrat indique le numéro du bon de commande, mais la facture de consommation (pay as you go) n'indique pas le numéro du bon de commande. Le pay-as-you-go modèle ne prend pas en charge l'ajout de numéros de bon de commande. Envisagez d'ajouter un bon de commande AWS Marketplaceavec une rubrique d'utilisation globale dans la AWS Billing console.
Bon de commande suspendu	Lorsqu'un numéro de bon de commande est fourni et que le bon de commande est marqué comme suspendu dans le tableau de bord des bons de commande de la console de facturation et de gestion des coûts, la nouvelle ligne est ajoutée au bon de commande, mais la facture n'inclut pas le bon de commande. L'administrateur de facturation Compte AWS doit activer le bon de commande et le contacter AWS Support pour régénérer la facture avec le bon de commande actif.
Bon de commande expiré	Lorsqu'un numéro de bon de commande est fourni et que le bon de commande arrive à expiration, le nouvel article est créé et le bon de commande est marqué comme actif. La date de fin de la ligne est utilisée comme date d'expiration du nouveau bon de commande.
Suivi du solde	Le suivi du solde n'est pas activé pour les AWS Marketplace rubriques.
Intégration du système d'approvisionnement	Le bon de commande fourni par un système d'approvisionnement intégré est indiqué sur les factures.

Scénario	Détails
Calendrier de paiement flexible - achat initial	Un contrat qui comporte des dates de facturation spécifiques (calendrier de paiement flexible) génère une ligne initiale dans le bon de commande pour zéro dollar. Des rubriques supplémentaires avec les prix applicables sont créées pour chaque facture.
Calendrier de paiement flexible - plusieurs bons de commande	Si vous avez besoin de vos paiements individuels pour qu'un calendrier de paiement flexible apparaisse avec différents bons de commande, contactez-nous AWS Support pour modifier le numéro du bon de commande sur les factures futures.

Informations sur les remboursements

Les clients peuvent demander différents types de remboursements pour lesAWS Marketplace produits. Pour lesAWS Marketplace produits vendus parAWS, consultez la page de la politique de remboursement, puis soumettez le formulaire de contact à l'aide duAWS Support Center Console. Si le produit est vendu par un tiers, consultez les politiques de remboursement sur la page détaillée du produit. Les frais logiciels pour lesAWS Marketplace abonnements sont payés au vendeur du produit, et les remboursements doivent être demandés directement au vendeur. ChaqueAWS Marketplace vendeur est tenu d'inclure une politique de remboursement sur saAWS Marketplace page.

Pour de plus amples informations sur les remboursements liés à vosAWS Marketplace achats, veuillez consulter les rubriques suivantes dans le Guide duAWS Marketplace vendeur :

- Remboursements
- Tarification du produit

> **Note**
>
> Pour tous les remboursements liés à des offres privées, contactez le vendeur.

Annulation de votre abonnement à un produit

Vous pouvez annuler votre abonnement à un produit ou le renouveler automatiquement dansAWS Marketplace. Les étapes suivantes fournissent des instructions pour les produits Software as a Service (SaaS), d'apprentissage automatique (ML) et Amazon Machine Image (AMI) dansAWS Marketplace.

Rubriques

Annulation de votre abonnement SaaS

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Accédez à la page Gérer les abonnements.
3. Pour le mode de livraison, choisissez SaaS dans la liste déroulante.
4. Sélectionnez l'abonnement pour le produit que vous souhaitez annuler.
5. Choisissez Cancel subscription (Annuler l'abonnement).

Annulation de votre abonnement à l'apprentissage automatique

Avant d'annuler votre abonnement de machine learning, effectuez les actions suivantes :

- Pour les algorithmes de machine learning : connectez-vous à la SageMaker console AmazonAWS Management Console et ouvrez-la. Mettez fin à toutes les tâches d'entraînement en cours pour votre algorithme. Si vous avez créé un package de modèles à partir de votre algorithme, vous ne pouvez pas lancer de point de terminaison en temps réel ni créer de tâche d'inférence par lots après l'annulation de votre abonnement au machine learning.
- Pour les packages de modèles de machine learning ou les modèles créés à partir de vos algorithmes, connectez-vous à la SageMaker console AmazonAWS Management Console et ouvrez-la. Mettez fin à tous les points de terminaison en temps réel de vos modèles ou interrompez toutes les tâches d'inférence par lots en cours d'exécution.

> **Note**
>
> Les tâches et les points de terminaison existants qui ne sont pas résiliés continueront à fonctionner et seront facturés jusqu'à leur résiliation.

Pour annuler un abonnement de machine learning

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Accédez à la page Mes abonnements.
3. Sélectionnez l'abonnement pour le produit que vous souhaitez annuler.
4. Choisissez Cancel subscription (Annuler l'abonnement). Après avoir annulé votre abonnement, vous ne pouvez pas lancer votre algorithme ou votre modèle.

Annulation de votre abonnement AMI

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Accédez à la page Gérer les abonnements.
3. Pour le mode de livraison, choisissez Amazon Machine Image dans la liste déroulante.
4. Sélectionnez l'abonnement pour le produit que vous souhaitez annuler.
5. Dans la liste déroulante Actions, choisissez Annuler l'abonnement.
6. Lisez les informations fournies pour confirmer que les instances en cours d'exécution sont facturées sur votre compte et cochez la case. Choisissez Oui, annuler l'abonnement.
7. Sélectionnez la cause deAWS la console dans un nouvel onglet.
8. Mettez fin à l'instance en cours d'exécution dans la console Amazon EC2. Si plusieurs instances sont en cours d'exécution, vous devez toutes les arrêter. Vous devez également supprimer lesAWS CloudFormation piles, le cas échéant.
9. Revenez à l'onglet Gérer les abonnements et choisissez Oui, Annuler l'abonnement. Après avoir annulé votre abonnement, vous perdez l'accès au logiciel et celui-ci ne sera plus facturé.

Annuler le renouvellement automatique de votre abonnement à un contrat SaaS

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Accédez à la page détaillée du produit.
3. Choisissez Continuer pour accéder à la page de commande.
4. Choisissez l'onglet Modifier le renouvellement, puis choisissez Annuler le renouvellement.

Moyens de paiement

Lorsque vous avez créé votre compte pour la première foisCompte AWS, vous avez défini le mode de paiement pour ce compte. Vous pouvez gérer vos modes de paiement dans la console AWS Billing and Cost Management. Pour obtenir des instructions, consultez la section Gestion de vos paiements dans le Guide de AWS Billing l'utilisateur.

Erreurs de paiement

Si une erreur se produit lors du traitement de votre paiement via votre compte payeur, mettez à jour votre mode de paiement et réessayez. Des erreurs peuvent se produire pour les raisons suivantes :

- Le mode de paiement est manquant, non valide ou non pris en charge.
- Le paiement a été refusé.
- Votre compte Amazon Internet Services Private Limited (AISPL) limite l'utilisation des cartes de débit ou de crédit pour les nouveaux achats selon un modèle de tarification contractuelle. Si vous possédez un compte AISPL, contactez le service client AWS pour mettre à jour votre mode de paiement par défaut. Pour plus de détails, consultez la section Restriction sur les achats par carte de crédit et de débit pour les clients de l'AISPL utilisant AWS Marketplace le site Web du AWS Marketplace blog.
- Votre offre privée inclut un calendrier de paiement. Toutefois, votre mode de paiement par défaut n'est pas configuré selon les conditions de facturation.

Les modes de paiement mis à jour peuvent prendre jusqu'à 7 jours pour être disponibles pour les nouveaux achats. Pour obtenir de l'aide concernant la résolution des problèmes, contactez AWS Support.

Devises prises en charge

Les listes suivantes incluent toutes les devises actuellement prises en charge pour AWS Amazon Web Services EMEA SARL.

> **Note**
>
> La roupie indienne (INR) n'est pas prise en charge car Amazon Internet Services Private Limited (AISPL) n'est pas prise en charge actuellement surAWS Marketplace. Pour plus d'informations, voir Quelles sont les différences entre les comptes Comptes AWS et les comptes AISPL.

Les devises prises en charge pour Amazon Web Services sont les suivantes :

- Dollar australien (AUD)
- Livre sterling (GBP)
- Dollar canadien (CAD)
- Couronne danoise (DKK)
- Euro (EUR)
- Dollar de Hong Kong (HKD)
- Yen japonais (JPY)
- Dollar néo-zélandais (NZD)
- Couronne norvégienne (NOK)
- Dollar de Singapour (SGD)
- Rand sud-africain (ZAR)
- Couronne suédoise (SEK)
- Franc suisse (CHF)
- Dollar américain (USD)

Les devises prises en charge par Amazon Web Services EMEA SARL sont les suivantes :

- Livre sterling (GBP)
- Couronne danoise (DKK)

- Euro (EUR)
- Couronne norvégienne (NOK)
- Rand sud-africain (ZAR)
- Couronne suédoise (SEK)
- Franc suisse (CHF)
- Dollar américain (USD)

Changer la devise de votre choix

Vos AWS Marketplace achats sont affichés dans la devise que vous avez spécifiée pour votreCompte AWS. Vous pouvez modifier la devise que vous préférez pour votre compte dans la AWS Billing and Cost Managementconsole. Pour obtenir des instructions, consultez la section Modification de la devise que vous utilisez pour payer votre facture dans le Guide de AWS Billing l'utilisateur.

> **Note**
>
> La modification de votre devise préférée modifie vos instructions de versement. Pour consulter les instructions de versement mises à jour, consultez votre AWS Marketplace facture ou consultez la page Paramètres du compte dans la AWS Billing and Cost Management console.

Mettre à jour les instructions de versement

Les clients Comptes AWS basés en Europe, au Moyen-Orient et en Afrique (EMEA), à l'exception de la Turquie et de l'Afrique du Sud, qui ont acheté des produits logiciels auprès de vendeurs éligibles à la zone EMEA reçoivent une facture d'Amazon Web Services EMEA SARL. Les factures Amazon Web Services EMEA SARL (AWSEurope) comportent des instructions de versement différentes de celles deAWS, Inc. Vous pouvez trouver des informations de versement sur vos factures lorsque vous êtes connecté à la console. AWS Billing and Cost Management Les comptes bancaires répertoriés dans la partie de la facture relative aux informations de versement sont différents des comptes de AWS Cloud services achetés via Amazon Web Services EMEA SARL. Amazon Web Services EMEA SARL utilise Amazon Payments Europe, S.C.A., un établissement de monnaie électronique agréé au Luxembourg, comme processeur de paiement pour les factures.

AWS Marketplace Toutes les factures doivent être réglées dans leur intégralité. Tout paiement ne couvrant pas le montant total de la facture sera remboursé sur votre compte bancaire.

Le tableau suivant décrit les types de transactions, l'entité effectuant la transaction et les instructions de versement correspondantes (nom du compte indiqué sous Détails du transfert électronique de fonds sur la facture).

Type de transaction	Entité commerçante	Instructions de versement
AWS Cloudachats de services	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
AWS MarketplaceVendeur éligible	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
Vendeur non éligible AWS Marketplace	AWSInc.	AWS

Pour demander une lettre bancaire contenant les instructions de versement, sélectionnez Facturation ou assistance relative aux comptes et créez un dossier d'assistance concernant le compte et la facturation sur Contact AWS ou envoyez un e-mail à `<awslux-receivables-support@email>` .amazon.com.

Pour plus d'informations sur la manière de modifier votre préférence de devise en faveur d'une devise prise en charge, consultez la section Modification de la devise que vous utilisez pour payer votre facture dans le Guide de AWS Billing l'utilisateur.

Amazon Web Services EMEA SARL accepte les paiements par transfert électronique de fondsMasterCard, par cartes de crédit VISA et American Express. Les cartes de crédit Diner's Club ou Discover ne sont pas acceptées.

Pour plus d'informations, consultez AWS Marketplacel'aide fiscale pour les acheteurs.

Balisage de répartition des coûts

AWS Marketplaceprend en charge le balisage de la répartition des coûts pour les produits logiciels que vous achetez. Vous pouvez utiliser des balises de répartition des coûts activées pour identifier et suivre l'utilisationAWS Marketplace des ressources viaAWS Cost Explorer des rapports deAWS coûts et d'utilisation,AWS des budgets ou d'autres outils d'analyse des coûts dans le cloud. Pour faciliter le classement et le suivi de vosAWS Marketplace coûts, et vous en sert pour organiser les coûts dans votre rapport de répartition des coûts.

Les étiquettes de répartition des coûtsAWS Marketplace proviennent des deux sources suivantes :

- Les coûts des produits logiciels d'Amazon Machine Image (AMI) qui sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) avec des balises héritent de ces mêmes balises. Vous pouvez activer ces balises en tant que balises de répartition des coûts dans laAWS Billing and Cost Management console pour un compte. Pour plus d'informations sur l'utilisation des balises de répartition des coûts avec les produits AMI, consultezMarquage de la répartition des coûts dans les produits AMI.
- Les produits AMI, les conteneurs et les logiciels en tant que service (SaaS) peuvent comporter des balises fournies par le fournisseur. Par exemple, un produit SaaS qui facture en fonction du nombre d'utilisateurs pourrait utiliser une étiquette pour identifier l'utilisation par service. Pour en savoir plus sur l'utilisation de ces balises, dans la pageÉtiquettes fournies par le fournisseur.

Le Identipour l'allocation des coûts ne fait le suivi des coûts qu'à partir du moment où les activer dans la console de Billing and Cost Management. SeulsCompte AWS les propriétaires, les propriétaires de comptes deAWS Organizations gestion et les utilisateurs disposant des autorisations appropriées peuvent accéder à la console de Billing and Cost Management d'un compte. Que vous utilisiez ou non le balisage de répartition des coûts, le montant qui vous est facturé reste inchangé. Le fait que vous utilisiez des balises de répartition des coûts n'a aucune incidence sur les fonctionnalités de vos produitsAWS Marketplace logiciels.

Pour les abonnements des vendeurs éligibles à la zone EMEA, le rapport sur les coûts et l'utilisation inclut une colonne pour la partieAWS contractante (Amazon Web Services EMEA SARL).

Étiquettes fournies par le fournisseur

AWS Marketplaceles produits dotés d'un système de mesure du fournisseur (y compris les produits AMI, les conteneurs et les produits SaaS) peuvent comporter des balises fournies par le fournisseur

de logiciels en tant que service supplémentaire pour ses clients. Ces balises sont des balises de répartition des coûts qui vous aident à comprendre l'utilisation de vosAWS Marketplace ressources en fonction des indicateurs fournis par les fournisseurs. Vous pouvez utiliser ces balises pour identifier et suivre l'utilisationAWS Marketplace des ressources viaAWS Cost Explorer Service,AWS Cost and Usage ReportAWS Budgets, ou d'autres outils d'analyse des coûts du cloud.

Les balises apparaissent sur votreAWS Billing console lorsque vous commencez à utiliser leAWS Marketplace produit et que le fournisseur envoie les relevés de comptage àAWS Marketplace. Si vous utilisez un produit sur la base d'un engagement initial dans le cadre d'un contrat, vous ne recevrez pas de mesure de la consommation du produit. Par conséquent, vous ne disposerez pas des balises définies par le fournisseur sur votreAWS Billing console. Si vous gérez un compte associé, vous devez disposer à la fois des`ViewBilling` autorisations`ModifyBilling` et des autorisations nécessaires pour afficher et activer les balisesAWS Billing. Pour plus d'informations, consultez les politiques relatives aux actions de facturation d'AWS dans le guide de l'utilisateur d'AWS Billing.

> **Note**
>
> L'activation des balises mesurées par le fournisseur peut augmenter la taille de votre rapport sur les coûts et l'utilisation. Votre rapport sur les coûts et l'utilisation est stocké dans Amazon S3. Par conséquent, vos coûts Amazon S3 pourraient également augmenter.

Pour activer les étiquettes personnalisées par le fournisseur pour tous lesAWS Marketplace produits éligibles

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Billing. Dans le volet de navigation de gauche de gauche de gauche de gauche de la page de navigation de gauche de gauche.
2. Dans l'onglet AWSde l'allocation des coûts générées par.
3. Recherchez pour`aws:marketplace:isv:` trouver les étiquettes de tous les produits compatibles avec le balisage défini par le fournisseur.
4. Activpour l'ensemble des pour l'allocation, puis puis puis puis puis puis Activpour l'activer. Vos étiquettes mesurées par le fournisseur entreront en vigueur dans les 24 heures.

Rubriques en relation

Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation des balises de répartition des coûts dans le Guide de l'utilisateur AWS Billing.
- Activation des balises de répartition des coûts générées par AWS dans le guide deAWS Billing l'utilisateur

Places de marché privées

Un marché privé contrôle les produits auprès desquels les utilisateurs de votre entrepriseCompte AWS, tels que les utilisateurs professionnels et les équipes d'ingénierie, peuvent se procurerAWS Marketplace. Il repose sur et permet à vos administrateurs de AWS Marketplace créer et de personnaliser des catalogues numériques organisés de fournisseurs de logiciels indépendants (ISV) approuvés et de produits conformes à leurs politiques internes. Les utilisateurs de votre entreprise Compte AWS peuvent trouver, acheter et déployer des produits approuvés sur votre place de marché privée, et s'assurer que tous les produits disponibles sont conformes aux politiques et aux normes de votre entreprise.

Un marché privé vous fournit un large catalogue de produits disponiblesAWS Marketplace, ainsi qu'un contrôle précis de ces produits. Vous pouvez ainsi centraliser la gestion de tous vos comptes, les regrouper en unités organisationnelles (UO) et associer différentes politiques d'accès à chaque UO. AWS Organizations Vous pouvez créer plusieurs expériences de marché privées associées à l'ensemble de votre organisation, à une ou plusieurs unités d'organisation ou à un ou plusieurs comptes de votre organisation, chacun disposant de son propre ensemble de produits approuvés. Vos AWS administrateurs peuvent également appliquer l'image de marque de l'entreprise à chaque expérience de marché privée avec le logo, le message et la palette de couleurs de votre entreprise ou de votre équipe.

Cette section décrit l'utilisation d'un marché privé en tant qu'acheteur. Pour plus d'informations sur la gestion des sites de vente privés en tant qu'administrateur, consultezCréation et gestion d'une place de marché privée.

Remarques

- Vous pouvez ajouter des produits privés qui ont été partagés avec vous (par le biais d'une offre privée) sur un marché privé. Pour plus d’informations, consultez Abonnement à un produit privé sur un marché privé .
- Sur un marché privé, les clients ont automatiquement droit à tous les produits dont les EULA sont régis par le contrat AWS client ou par un autre accord AWS régissant l'utilisation deServices AWS. Les clients ont déjà droit à ces produits par défaut ; ils ne figurent donc pas dans la liste des produits que vous avez approuvés sur votre site de vente privé. Les clients peuvent utiliser Service Catalog pour gérer le déploiement de ces produits.

Affichage des pages détaillées du produit

Les utilisateurs ne peuvent s'abonner qu'aux produits que vous avez autorisés sur le marché privé qui régit le compte. Ils peuvent parcourir et consulter la page détaillée de n'importe quel produit, mais l'abonnement n'est activé que pour les produits que vous avez ajoutés à votre place de marché privée. Si un produit ne figure pas actuellement sur votre site de vente privé, l'utilisateur voit une bannière rouge en haut de la page, indiquant que l'achat du produit n'a pas été approuvéAWS Marketplace.

Si les demandes logicielles sont activées, les utilisateurs peuvent choisir Créer une demande sur la page de détails du produit. Lorsque les utilisateurs choisissent Créer une demande, ils soumettent une demande à l'administrateur pour que le produit soit disponible sur votre place de marché privée. Pour en savoir plus sur cette fonction, consultez Gestion des demandes des utilisateurs.

S'abonner à un produit sur une place de marché privée

Pour vous abonner à un produit sur votre site de vente privé en tant qu'utilisateur, accédez à la page de détails du produit et choisissez Continuer. Cela vous redirige vers la page d'abonnement du produit. Sur la page d'abonnement, vous pouvez effectuer vos sélections de configuration, puis choisir Subscribe (S'abonner).

Si le produit n'est pas approuvé dans votre place de marché privée, Subscribe (S’abonner) n'est pas disponible. Une bannière rouge en haut de la page indique que le produit n'est pas approuvé pour l’achat. Si les demandes logicielles sont activées, vous pouvez choisir Create request (Créer une demande) pour soumettre une demande à votre administrateur afin que le produit soit ajouté à votre place de marché privée.

Abonnement à un produit privé sur un marché privé

Certains produits ne sont pas accessibles au publicAWS Marketplace. Ces produits ne sont visibles que lorsque le vendeur vous fait une offre privée. Toutefois, vous ne pouvez vous abonner que si l'administrateur de votre place de marché privée ajoute d'abord le produit à votre place de marché privée. Pour cette raison, l'offre privée doit être étendue à votre compte Compte AWS et à celui qui inclut l'administrateur du marché privé de votre organisation. Une fois que l'offre privée a été étendue à la fois à l'utilisateur et à l'administrateur, l'administrateur du marché privé peut ajouter le produit à votre place de marché privée. Une fois le produit approuvé, vous pouvez vous abonner au produit comme à n'importe quelle autre offre privée.

Demander l'ajout d'un produit à votre place de marché privée

En tant qu'utilisateur, vous pouvez demander à votre administrateur d'ajouter un produit qui ne figure pas sur votre place de marché privée. Pour effectuer une demande, accédez à la page des détails du produit, choisissez Create request (Créer une demande), formulez une demande à votre administrateur pour que le produit soit ajouté à votre place de marché privée, puis soumettez votre demande. Pour suivre l'état de votre demande, dans le menu déroulant de gauche, sélectionnez Your Private Marketplace Requests (Vos demandes Private Marketplace).

Création et gestion d'une place de marché privée

Pour créer et gérer un marché privé, vous devez être connecté au compte de gestion ou au compte d'administrateur délégué du marché privé. Vous devez également disposer des autorisations AWS Identity and Access Management (IAM) définies dans la politique AWSPrivateMarketplaceAdminFullAccess IAM. Pour plus d'informations sur l'application de cette politique aux utilisateurs, aux groupes et aux rôles, consultezthe section called “Création d'un administrateur de marché privé”.

> **Note**
>
> Si vous êtes actuellement client d'un marché privé sans AWS Organizations intégration d'un marché privé, vous pouvez créer et gérer un marché privé à partir de n'importe quel compte de votre organisation doté de la politique AWSPrivateMarketplaceAdminFullAccess IAM.

Cette section inclut les tâches que vous pouvez effectuer en tant qu'administrateur du marché privé via le AWS Marketplace site Web. Vous pouvez également gérer des places de marché privées à l'aide duAWS Marketplace Catalog API. Pour plus d'informations, consultez la section Travailler avec un marché privé dans la AWS Marketplace Catalog APIréférence.

Débuter avec le marché privé

Pour commencer à utiliser Private Marketplace, assurez-vous d'être connecté à votre compte AWS de gestion, accédez à Private Marketplace, puis activez les prérequis suivants :

- Accès sécurisé : vous devez activer l'accès sécurisé pourAWS Organizations, ce qui permet au compte de gestion d'une organisation de fournir ou de révoquer l'accès à ses AWS Organizations

données pour un AWS service. L'activation d'un accès sécurisé est essentielle pour que le marché privé s'intègre au marché privé AWS Organizations et le désigne comme un service fiable au sein de votre organisation.

- Rôle lié à un service : vous devez activer le rôle lié à un service du marché privé, qui réside dans le compte de gestion et inclut toutes les autorisations requises par le marché privé pour décrire AWS Organizations et mettre à jour les ressources du marché privé en votre nom. Pour plus d'informations sur le rôle lié à un service, consultez Utiliser des rôles pour configurer Private Marketplace dans. AWS Marketplace

> **Note**
>
> Les clients actuels de Private Marketplace peuvent activer les paramètres de votre place de marché privée en accédant à la page d'administration de Private Marketplace et en choisissant Paramètres. En activant un accès sécurisé AWS Organizations et en créant un rôle lié à un service, vous pouvez utiliser des fonctionnalités telles que l'association d'unités d'organisation à des expériences de marché privées et l'enregistrement d'un administrateur délégué. Lorsque cette option est activée, seuls le compte de gestion et le compte d'administrateur délégué peuvent créer et gérer des expériences de marché, les ressources existantes étant transférées vers le compte de gestion et partagées uniquement avec l'administrateur délégué. La désactivation de l'accès sécurisé supprimera la gouvernance du marché privé pour votre organisation. Aucun groupe de comptes n'est affiché sur votre place de marché privée. Pour consulter la gouvernance de votre organisation à différents niveaux, utilisez la page Structure de l'organisation. Pour toute question ou assistance, contactez-nous.

Gestion du marché privé

Vous pouvez gérer votre place de marché privée depuis la page d'administration de Private Marketplace, sous Paramètres, dans le volet de gauche. L'administrateur du compte de gestion et les administrateurs délégués peuvent utiliser cette page pour consulter les détails du marché privé, notamment le marché privé par défaut et le nombre d'expériences en direct.

Les administrateurs de comptes de gestion peuvent également utiliser cette page pour gérer les paramètres suivants.

Administrateurs délégués

L'administrateur du compte de gestion peut déléguer les autorisations administratives du marché privé à un compte membre désigné appelé administrateur délégué. Pour enregistrer un compte en tant qu'administrateur délégué pour le marché privé, l'administrateur du compte de gestion doit s'assurer que l'accès sécurisé et le rôle lié au service sont activés, choisir Enregistrer un nouvel administrateur, fournir le numéro de AWS compte à 12 chiffres et choisir Soumettre.

Les comptes de gestion et les comptes d'administrateur délégué peuvent effectuer des tâches administratives sur le marché privé, telles que la création d'expériences, la mise à jour des paramètres de marque, l'association ou la dissociation d'audiences, l'ajout ou la suppression de produits, ainsi que l'approbation ou le refus des demandes en attente.

Accès fiable et rôle lié au service

L'administrateur du compte de gestion peut activer les fonctionnalités suivantes pour votre place de marché privée.

> **Note**
>
> Les clients actuels de Private Marketplace peuvent activer les paramètres de votre place de marché privée en accédant à la page d'administration de Private Marketplace et en choisissant Paramètres. En activant un accès sécurisé AWS Organizations et en créant un rôle lié à un service, vous pouvez utiliser des fonctionnalités telles que l'association d'unités d'organisation à des expériences de marché privées et l'enregistrement d'un administrateur délégué. Lorsque cette option est activée, seuls le compte de gestion et le compte d'administrateur délégué peuvent créer et gérer des expériences de marché, les ressources existantes étant transférées vers le compte de gestion et partagées uniquement avec l'administrateur délégué. La désactivation de l'accès sécurisé supprimera la gouvernance du marché privé pour votre organisation. Aucun groupe de comptes n'est affiché sur votre place de marché privée. Pour consulter la gouvernance de votre organisation à différents niveaux, utilisez la page Structure de l'organisation. Pour toute question ou assistance, contactez-nous.

- Accès sécurisé : vous devez activer l'accès sécurisé pourAWS Organizations, ce qui permet au compte de gestion d'une organisation de fournir ou de révoquer l'accès à ses AWS Organizations données pour un AWS service. L'activation d'un accès sécurisé est essentielle pour que le marché

privé s'intègre au marché privé AWS Organizations et le désigne comme un service fiable au sein de votre organisation.

- Rôle lié à un service : vous devez activer le rôle lié à un service du marché privé, qui réside dans le compte de gestion et inclut toutes les autorisations requises par le marché privé pour décrire AWS Organizations et mettre à jour les ressources du marché privé en votre nom. Pour plus d'informations sur le rôle lié à un service, consultez Utiliser des rôles pour configurer Private Marketplace dans. AWS Marketplace

Création d'une expérience de marché privée

Votre place de marché privée est composée d'une ou de plusieurs expériences de marché privées. Une expérience peut être associée à l'ensemble de votre organisation, à une ou plusieurs unités d'organisation ou à un ou plusieurs comptes de votre organisation. Si vous Compte AWS n'êtes pas membre d'une organisation, vous disposez d'une expérience de marché privée associée à un compte. Pour créer votre place de marché privée, accédez à Private Marketplace, sélectionnez la page Expériences sur la gauche, puis choisissez Create experience.

> **Note**
>
> Pour utiliser le marché privé avecAWS Organizations, vous devez activer toutes les fonctionnalités de l'organisation. Pour de plus amples informations, consultez Activation de toutes les fonctionnalités de l'organisation dans le Guide de l'utilisateur AWS Organizations. Si vous Compte AWS n'êtes pas membre d'une organisation, vous n'avez besoin d'aucune étape préalable pour utiliser le marché privé.

Votre expérience de marché privée est créée sans produits approuvés, sans éléments de marque et n'est associée à aucun compte au sein de votre organisation. Il n'est pas en ligne par défaut. Les rubriques suivantes décrivent comment utiliser votre expérience de marché privé.

Ajouter des produits à votre expérience de marché privé

Pour ajouter des produits à une expérience de marché privée

1. Sur la page de l'administrateur de Private Marketplace, sélectionnez Experiences dans le volet de navigation de gauche. Ensuite, dans l'onglet Produits, sélectionnez Tous les produits AWS Marketplace. Vous pouvez effectuer une recherche par nom de produit ou par nom de vendeur.

2. Cochez la case en regard de chaque produit à ajouter à votre Private Marketplace, puis choisissez Add to Private Marketplace (Ajouter à Private Marketplace).

> **Note**
>
> Vous pouvez également ajouter un produit directement depuis la page détaillée du produit en cliquant sur le bouton Add to Private Marketplace sur le bandeau rouge. Si le bandeau rouge ne figure pas sur la page détaillée du produit, celui-ci se trouve déjà sur votre site de vente privé.

Vous pouvez également ajouter plusieurs produits à plusieurs expériences à la fois en choisissant Ajouter/supprimer des produits en bloc dans le volet de navigation de gauche.

Vérification des produits dans le cadre de votre expérience de marché privée

Pour vérifier qu'un produit est approuvé dans le cadre de votre expérience de marché privé

1. Sur la page de l'administrateur de Private Marketplace, sélectionnez Experiences dans le volet de navigation de gauche.
2. Choisissez des produits approuvés. Tous les produits approuvés apparaissent dans la liste des produits approuvés.

> **Note**
>
> Si vous utilisez un compte associé à l'expérience que vous modifiez et que celle-ci est activée, vous pouvez également consulter les produits directement dans la AWS Marketplace console (https://console.aws.amazon.com/marketplace). Tous les produits figurant dans les résultats de recherche affichent un badge d'achat approuvé s'ils font partie de votre site de vente privé.

Personnalisation de votre expérience de marché privé

Les expériences sont des sous-ensembles de produits et de marques associées qui peuvent avoir un ou plusieurs publics associés. Une seule expérience de marché privé peut régir l'ensemble de l'organisation si l'expérience est associée à l'organisation ou si elle régit un ou plusieurs comptes ou unités organisationnelles de votre organisation.

Vous pouvez gérer les paramètres de votre expérience depuis la page d'administration de Private Marketplace, sous Experiences, dans le volet de gauche. Utilisez cette page pour consulter et gérer toutes vos expériences actives et archivées et pour créer de nouvelles expériences pour votre place de marché privée. Pour chaque expérience, vous pouvez ajouter un logo, ajouter un titre et personnaliser l'interface utilisateur afin d'utiliser le schéma de couleurs de votre organisation.

Gérer les audiences

Une audience est une organisation ou un groupe d'unités organisationnelles (UO) ou de comptes que vous pouvez associer à une expérience de marché privée. Vous pouvez créer une audience depuis la page d'administration de Private Marketplace, sous Experiences, dans le volet de gauche.

Vous pouvez associer une ou plusieurs audiences à une expérience. Lorsque vous associez ou dissociez une audience, cela peut modifier l'expérience de gouvernance des UO et des comptes enfants. Utilisez la page Structure de l'organisation pour voir les comptes et les unités d'organisation concernés par l'association. Si vous désactivez l'accès sécurisé, vos audiences seront dissociées et toute gouvernance supprimée.

> **Note**
>
> Vous pouvez consulter votre AWS Organizations hiérarchie et gérer la gouvernance de votre organisation à partir d'un marché privé. Pour gérer votre place de marché privée au niveau de l'unité organisationnelle et enregistrer les administrateurs délégués, activez l'accès sécurisé et le rôle lié au service depuis la page Paramètres. Pour toute question ou assistance, contactez-nous.

Configuration de votre place de marché privée

Une fois que vous êtes satisfait de la liste des produits de l'expérience, des paramètres de marque de la place de marché et des groupes de comptes associés, vous pouvez lancer votre place de marché privée. Sur la page de l'administrateur de AWSPrivate Marketplace, sélectionnez Experience dans

le volet de navigation de gauche, puis sélectionnez l'expérience que vous souhaitez activer. Dans l'onglet Paramètres, vous pouvez modifier le statut du marché privé entre En ligne (activé) et Non en ligne (désactivé).

Vous pouvez également choisir d'autoriser les utilisateurs à soumettre des demandes de logiciels avec des demandes de logiciels. Si les demandes de logiciels sont activées (activées), les utilisateurs finaux peuvent choisir Créer une demande sur la page de détails du produit pour soumettre une demande à l'administrateur afin que le produit soit disponible sur votre place de marché privée. Les demandes de logiciels sont activées par défaut et le paramètre ne peut être modifié que lorsque le marché privé est activé.

Lorsque votre place de marché privée est en ligne, les utilisateurs finaux ne peuvent acheter que les produits que vous avez approuvés. Lorsque votre place de marché privée est désactivée, vous conservez la liste des produits. Toutefois, la désactivation d'un marché privé supprime cette restriction pour les utilisateurs de votre AWS Organizations organisation. Par conséquent, ils peuvent s'abonner à tous les produits destinés au publicAWS Marketplace.

La mise en ligne d'une place de marché privée ne perturbe pas l'exécution active d'Amazon Machine Images (AMI) sur les instances Amazon Elastic Compute Cloud (Amazon EC2). Il est recommandé de veiller à ce que tous les AWS Marketplace produits actuellement utilisés au sein de votre entreprise soient inclus dans votre marché privé. Il est également recommandé de mettre en place un plan visant à mettre fin à l'utilisation de produits non approuvés avant de lancer le marché privé. Une fois le marché privé en ligne, tous les nouveaux abonnements ou renouvellements sont régis par les produits approuvés dans le catalogue du marché privé.

Travailler avec des produits privés

Certains produits ne sont pas accessibles au publicAWS Marketplace. Ces produits ne sont visibles que lorsque le vendeur vous fait une offre privée. L'offre privée du vendeur inclut un lien vers le produit. Vous pouvez ajouter le produit au marché privé à partir de la bannière en haut de la page.

> **Note**
>
> Si vous souhaitez vous abonner à un produit privé à partir d'un autre compte au sein de votre organisation, le vendeur doit inclure à la fois votre compte Compte AWS (pour ajouter le produit sur le marché privé) et le compte de l'utilisateur (pour souscrire au produit) dans l'offre privée.

Pour supprimer un produit privé de votre place de marché privée, vous devez contacter le AWS Marketplace Support.

Gestion des demandes des utilisateurs

Vous pouvez autoriser les utilisateurs à soumettre des demandes pour que des produits soient ajoutés à leur catalogue de marché privé à l'aide de la fonctionnalité de demande de logiciel. Pour ce faire, accédez à la page d'administrateur de votre place de marché privée, sélectionnez Expériences dans le volet de navigation de gauche, puis choisissez l'expérience que vous souhaitez gérer. Dans l'onglet Produits, sélectionnez Demandes en attente. De là, vous pouvez consulter les demandes faites par vos utilisateurs pour que des produits soient ajoutés à leur catalogue de marché privé.

Vous pouvez ajouter n'importe quel nombre de produits demandés à partir de cette page en cochant d'abord la case en regard du nom de chaque produit demandé, puis en sélectionnant Add to Private Marketplace (Ajouter à la place de marché privée). De même, vous pouvez également refuser une ou plusieurs demandes sélectionnées en choisissant Decline (Refuser). Pour afficher plus d'informations sur un produit (ou sa demande logicielle), choisissez Afficher les détails dans la colonne Détails de cette demande.

Lorsque vous refusez une demande de produit, vous pouvez ajouter une raison et empêcher de futures demandes (bloquer) pour ce produit. Le blocage d'un produit ne vous empêchera pas de l'ajouter à votre place de marché privée, mais cela empêchera vos utilisateurs de demander le produit.

Archivage et réactivation d'une expérience de marché privée

Vous pouvez supprimer une expérience de marché privée en l'archivant. Les expériences archivées ne peuvent pas être mises à jour ni utilisées pour gérer les comptes de votre organisation. Si des audiences sont associées à une expérience archivée, vous pouvez les associer à une autre expérience. Si vous décidez d'utiliser l'expérience ultérieurement, vous pouvez toujours la réactiver. Les administrateurs de comptes de gestion ou les administrateurs délégués sont autorisés à archiver et à réactiver les expériences.

> **Note**
>
> Avant d'archiver une expérience, vous devez la désactiver. Pour plus d'informations sur la désactivation d'une expérience, consultez Configuration de votre place de marché privée.

Si vous êtes actuellement client d'une place de marché privée sans AWS Organizations intégration d'une place de marché privée, les administrateurs du compte qui a créé l'expérience sont autorisés à archiver et à réactiver les expériences.

Pour archiver une ou plusieurs expériences de marché privées

1. Sur la page de l'administrateur de Private Marketplace, sélectionnez Experiences dans le volet de navigation de gauche.
2. Dans l'onglet Expériences actives, sélectionnez une ou plusieurs expériences.
3. Choisissez Archiver Experience.

> **Note**
>
> Si une ou plusieurs expériences ont le statut Live, vous devez les mettre hors ligne en choisissant Mettre les expériences hors ligne.

4. Pour vérifier que vous souhaitez archiver l'expérience, tapez **`confirm`** (en minuscules) dans la zone de texte.
5. Choisissez Archive (Archiver).

> **Note**
>
> Vous pouvez également archiver une expérience en la sélectionnant, en choisissant Archiver l'expérience sous Mode administrateur dans l'onglet Paramètres, puis en choisissant Enregistrer.

Pour réactiver une ou plusieurs expériences de marché privé

1. Sur la page de l'administrateur de Private Marketplace, sélectionnez Experiences dans le volet de navigation de gauche.
2. Dans l'onglet Expériences archivées, sélectionnez une ou plusieurs expériences.
3. Choisissez Réactiver.
4. Pour vérifier que vous souhaitez réactiver l'expérience, tapez **`confirm`** dans la zone de texte.
5. Choisissez Réactiver.

> **Note**
>
> Vous pouvez également réactiver une expérience en la sélectionnant, en choisissant Réactiver l'expérience en mode administrateur dans l'onglet Paramètres, puis en choisissant Enregistrer.

Offres privées

La fonctionnalité d'offre privée du AWS Marketplace vendeur vous permet de recevoir les prix des produits et les conditions du CLUF d'un vendeur qui ne sont pas accessibles au public. Vous négociez la tarification et les conditions avec le vendeur, puis il crée une offre privée pour le compte AWS de votre choix. Vous devez accepter l'offre privée avant de commencer à bénéficier du prix et des conditions d'utilisation négociés.

Pour chaque offre privée, votre compte bénéficie d'une tarification et de conditions de licence spécifiques. Le vendeur du produit vous donne accès à une offre privée associée à une date d'expiration définie. Si vous n'acceptez pas l'offre privée avant la date d'expiration, selon le type de produit faisant l'objet de l'offre privée, vous êtes automatiquement redirigé vers l'offre publique du produit ou êtes désabonné du produit.

Si vous utilisez la fonctionnalité de facturation consolidée dansAWS Organizations, vous pouvez accepter l'offre privée depuis le compte de gestion de l'organisation ou depuis le compte d'un membre. Si vous acceptez depuis le compte de gestion, l'offre privée peut être partagée avec tous les comptes membres de l'organisation. Les comptes membres précédemment abonnés au produit doivent également accepter la nouvelle offre privée afin de bénéficier de la tarification. Pour les produits AMI et Container, vous pouvez également partager la licence entre le compte de gestion et les comptes des membres à l'aide de AWS License Manager. Les comptes membres qui n'étaient pas abonnés au produit auparavant doivent accepter l'offre privée pour pouvoir déployer le produit.

Pour plus d'informations sur la facturation consolidée, consultez la section Consolidated Billing for Organizations dans le guide de AWS Billing l'utilisateur. Voici des points clés à retenir lorsque vous commencez à utiliser vos offres privées.

- AWS Marketplaceles acheteurs peuvent accéder à des services de financement tiers pour des offres privées. Pour plus d'informations, voir Le financement à la clientèle est désormais disponible dans AWS Marketplace.
- Il n'y a aucune différence dans le produit logiciel que vous achetez au moyen d'une offre privée. Le logiciel que vous achetez au moyen d'une offre privée fonctionne de la même façon que si vous l'aviez acheté sans offre privée.
- Les abonnements aux produits que vous achetez avec une offre privée s'affichent comme n'importe quel autre produit AWS Marketplace sur votre facture mensuelle. Vous pouvez également utiliser la facturation détaillée pour afficher l'utilisation de chaque produit

AWS Marketplace acheté. Pour chacune de vos offres privées, une ligne correspond à chaque type d'utilisation.

- Vous n’avez pas besoin de lancer une nouvelle instance du logiciel pour vous abonner à une offre privée. Lorsque vous acceptez une offre privée, le prix est modifié afin de correspondre au prix de l’offre privée. Si le lancement 1-Click est proposé pour un produit, vous pouvez déployer une nouvelle instance du logiciel. Si un produit effectue par défaut un lancement 1-click, vous pouvez accepter une offre privée sans lancer une nouvelle instance. Pour effectuer un lancement sans déployer de nouvelle instance, choisissez Manual Launch (Lancement manuel) sur la page de commande. Vous pouvez utiliser la console Amazon Elastic Compute Cloud pour déployer des instances supplémentaires, comme vous le feriez pour d'autres AWS Marketplace produits.
- Lorsqu’un vendeur vous propose une offre privée, vous recevez la confirmation sur le compte inclus par le vendeur dans l'offre privée. Les offres privées sont liées au compte de l'acheteur du logiciel défini. Le vendeur du logiciel crée l'offre privée pour le compte que vous spécifiez. Chaque offre privée peut être envoyée vers 25 comptes maximum.
- Lorsque vous acceptez une offre privée, elle devient un contrat (également appelé contrat ou abonnement) entre vous et le vendeur.
- Les vendeurs peuvent proposer de mettre à niveau ou de renouveler votre achat d'un contrat SaaS ou d'un contrat SaaS avec un produit de consommation. Par exemple, un vendeur peut créer une nouvelle offre privée pour octroyer de nouveaux droits, proposer des remises tarifaires, ajuster les échéanciers de paiement ou modifier le contrat de licence utilisateur final (CLUF) pour utiliser des conditions de licence standardisées.

  Ces renouvellements ou mises à niveau sont des modifications apportées à l'offre privée d'origine que vous avez acceptée, et vous utilisez le même processus pour les accepter. Si vous acceptez la nouvelle offre privée de mise à niveau ou de renouvellement, les nouvelles conditions du contrat prennent effet immédiatement, sans interruption du service logiciel. Toutes les conditions antérieures ou les paiements prévus restants sont annulés et remplacés par les conditions de cette nouvelle entente.
- Vous pouvez consulter l'ensemble de vos abonnements annuels dans AWS Marketplace sous la page Your Software (Vos logiciels). Si un abonnement annuel est acheté à l’aide d’un compte utilisant AWS Organizations pour la facturation consolidée, il est partagé par l'ensemble de la famille de comptes associés. Si aucune instance n’est exécutée sur le compte d'achat, l'abonnement annuel compte l'utilisation du logiciel exécuté sur un autre compte associé. Pour en savoir plus sur les abonnements annuels, consultez la page the section called “Abonnements AMI”.

- Vous ne pouvez pas vous abonner à une offre privée si elle a expiré. Vous pouvez toutefois contacter le vendeur. Demandez au vendeur de remplacer la date d'expiration de l'offre actuelle par une date future ou de créer une nouvelle offre privée pour vous.

Types de produits éligibles aux offres privées

Vous pouvez recevoir des offres privées pour les types de produits suivants.

Type d'offre	Description
Produits de données	Pour plus d'informations, consultez la section Acceptation d'une offre privée dans le guide de l'utilisateur d'AWS Data Exchange.
Contrat SaaS	Avec un contrat SaaS, vous pouvez vous engager à effectuer un paiement initial pour l'utilisation prévue d'un produit SaaS, ou négocier un calendrier de paiement flexible avec le vendeur. Les durées des contrats sont d'un mois, un an, deux ou trois ans, ou sélectionnez une durée personnalisée en mois, jusqu'à 60 mois. Si vous vous engagez à un paiement initial, vous êtes facturé à l'avance pour l'utilisation du logiciel du produit. Si le vendeur propose un calendrier de paiement flexible, vous êtes facturé selon les dates du calendrier de paiement selon les montants indiqués sur l'offre privée. Le vendeur peut également inclure des pay-as-you-go prix négociés pour une utilisation supérieure à l'utilisation prévue dans le contrat.
Abonnement SaaS	Avec un abonnement SaaS, vous acceptez un prix pour l'utilisation d'un produit. Le vendeur

Type d'offre	Description
	suit et signale votre utilisation à AWS Marketplace. Vous est facturé pour ce que vous utilisez.
AMI horaires	Avec les AMI horaires, vous négociez un tarif horaire pour l'utilisation d'une AMI, arrondie à l'heure la plus proche.
AMI toutes les heures et tous les ans	Avec AMI horaire et annuel, vous négociez les tarifs horaires et à long terme par type d'instance. La tarification à long terme est valable pour la durée de l'offre privée, qui peut être comprise entre 1 jour et 3 ans. Si le vendeur crée une offre privée sans calendrier de paiement flexible, vous pouvez exécuter des instances Amazon EC2 au prix horaire déterminé dans l'offre privée et éventuellement souscrire des engagements initiaux pour la durée du contrat au prix à long terme défini dans l'offre privée. Si le vendeur crée une offre privée avec un calendrier de paiement flexible, les dates du calendrier de paiement vous sont facturées pour les montants indiqués sur l'offre privée, quelle que soit l'utilisation. Dans ce type d'offre privée, le vendeur peut inclure un certain nombre d'instances Amazon EC2 par type d'instance que vous pouvez exécuter sans que le prix horaire ne vous soit facturé. Toute utilisation supérieure à ce qui est inclus est ensuite facturée au prix horaire fixé dans l'offre privée.

Type d'offre	Description
Contrat AMI	Avec les contrats AMI, vous négociez le prix du contrat et la durée du contrat, qui peut aller de 1 à 60 mois. Si le vendeur crée une offre privée sans calendrier de paiement flexible, au moment de l'acceptation, vous pouvez configurer le contrat en fonction du prix et des options définis dans l'offre privée. Si le vendeur crée une offre privée avec un calendrier de paiement flexible, les dates du calendrier de paiement vous sont facturées aux montants indiqués sur l'offre privée. Dans ce type d'offre privée, le vendeur configure le contrat dans l'offre privée et celui-ci ne peut pas être configuré au moment de l'acceptation.
Produits de conteneur	Pour les produits en conteneur, vous négociez le prix horaire ou annuel des produits en conteneur que vous utilisez, par module, tâche ou unité personnalisée, en fonction du produit que vous achetez. Les offres privées de produits en conteneur correspondent aux offres privées de produits AMI.
Produits de Machine Learning	Les offres privées peuvent être un contrat avec des frais initiaux fixes pour un nombre de jours spécifié. À la fin du contrat, toutes les instances qui continuent à fonctionner sont facturées au taux horaire défini par le vendeur dans l'offre privée.
Services professionnels	Toutes les offres de services professionnels sont des offres privées. Vous devez travailler avec l'acheteur pour créer l'offre privée. Pour plus d’informatons, consultez Produits de services professionnels.

Préparation préalable à l’acceptation d’une offre privée

Lorsqu'une offre privée typique est négociée, vous payez le montant total de l'offre lorsque vous l'acceptez, sauf si vous utilisez un financement tiers. Dans le cas du financement par un tiers, le financier paie le contrat en votre nom et vous facture en fonction du calendrier de paiement convenu. Avant d'accepter une offre privée, vérifiez la structure de facturation de votre entreprise, votre mode de paiement pour la facturation AWS et vos paramètres fiscaux.

Vérification de vos préférences AWS Billing and Cost Management

Billing and Cost Management est le service que vous utilisez pour payer votre AWS facture, surveiller votre utilisation et budgétiser vos coûts. Vous pouvez utiliser la fonctionnalité de facturation consolidée AWS Organizations pour consolider la facturation et le paiement de plusieurs comptes ou de plusieurs comptes Amazon Internet Services Pvt. Ltd (AISPL). Chaque organisation AWS Organizations possède un compte de gestion qui paie les frais de tous les comptes des membres. Le compte de gestion est appelé compte payeur, et le compte membre est appelé compte lié. Avant de négocier une offre privée, vérifiez comment votre entreprise paie sa AWS facture et AWS sur quel compte l'offre privée est faite.

Vérification de votre mode de paiement

Avant d'accepter une offre privée, vérifiez que votre mode de paiement est capable de prendre en charge l'intégralité du coût de l’offre privée. Pour vérifier votre mode de paiement, ouvrez la console Billing and Cost Management à l'adresse https://console.aws.amazon.com/billing/.

Vérification de vos paramètres fiscaux

Si votre entreprise a droit à une exonération fiscale, vérifiez vos paramètres fiscaux. Pour afficher ou modifier vos paramètres fiscaux, connectez-vous à la console AWS Management Console et accédez aux paramètres de votre compte. Pour en savoir plus sur l'enregistrement fiscal, consultez la page Comment ajouter ou mettre à jour mon numéro d'identification fiscale ou mon adresse commerciale légale pour mon compte AWS ?.

Affichage d’une offre privée et abonnement

Vous pouvez consulter une offre privée de l'une des manières suivantes :

Rubriques

- Consulter et souscrire à une offre privée à partir d'une liste d'offres privées

Consulter et souscrire à une offre privée à partir d'une liste d'offres privées

Pour consulter et souscrire à une offre privée à partir d'une liste d'offres privées étendues à votre Compte AWS

1. Connectez-vous à la console AWS Marketplace.
2. Accédez à la page des offres privées.
3. Sur la page Offres privées, sous l'onglet Offres disponibles, sélectionnez le numéro d'offre correspondant à l'offre qui vous intéresse.
4. Consultez l'offre privée et abonnez-vous à celle-ci.

Consulter et souscrire à une offre privée à partir d'un lien fourni par le vendeur

Pour consulter et souscrire à une offre privée à partir d'un lien que le vendeur vous a envoyé

1. Connectez-vous à la console AWS Marketplace.
2. Suivez le lien envoyé par le vendeur pour accéder directement à l'offre privée.

> **Note**
>
> Le fait de suivre ce lien avant de vous connecter au bon compte entraînera le message d'erreur « Page introuvable » (404).
> Pour plus d'informations, consultez Je reçois un message d'erreur Page introuvable (404) lorsque je clique sur l'ID de l'offre pour afficher l'offre privée.

3. Consultez l'offre privée et abonnez-vous à celle-ci.

Consulter et souscrire à une offre privée depuis la page du produit

Pour consulter et souscrire à une offre privée depuis la page du produit

1. Connectez-vous à la console AWS Marketplace.

2. Accédez à la page du produit.
3. Affichez la bannière en haut de la page indiquant l'offre privée, le numéro de l'offre et la date d'expiration de l'offre.

> **Note**
>
> Les offres privées à date future sont répertoriées dans la catégorie des renouvellements anticipés. Pour plus d'informations, consultez the section called “Travailler avec de futurs accords datés”.

4. Sélectionnez le numéro de l'offre.
5. Consultez l'offre privée et abonnez-vous à celle-ci.

> **Note**
>
> Si vous avez accès à plusieurs offres privées pour ce produit, chaque offre apparaît sous Offer name (Nom de l’offre). Si vous avez un contrat en cours pour ce produit, une icône en cours d'utilisation apparaît à côté de cette offre.

Résolution des problèmes liés aux offres privées

Si vous rencontrez des problèmes liés au code d'état HTTP 404 (Introuvable) ou si vous rencontrez des difficultés similaires lorsque vous utilisez des offres privéesAWS Marketplace, consultez les rubriques de cette section.

Problèmes

- Je reçois un message d'erreur Page introuvable (404) lorsque je clique sur l'ID de l'offre pour afficher l'offre privée
- Aucune de ces suggestions ne fonctionne

Je reçois un message d'erreur Page introuvable (404) lorsque je clique sur l'ID de l'offre pour afficher l'offre privée

- Vérifiez que vous êtes connecté correctementCompte AWS. Le vendeur étend les offres privées à des Compte AWS identifiants spécifiques.

- Vérifiez si l'offre existe sous Offres privées dans la AWS Marketplace console. Si vous ne trouvez pas l'offre dans la section Offres privées, cela peut être dû au fait que le vendeur l'a étendue à un autre Compte AWS identifiant. Vérifiez auprès du vendeur l'Compte AWSidentifiant auquel l'offre a été étendue.
- Vérifiez que l'offre privée n'a pas expiré en consultant l'onglet Offres acceptées et expirées sous Offres privées dans la AWS Marketplace console. Si l'offre a expiré, contactez le vendeur pour modifier la date d'expiration de l'offre ou étendre une nouvelle offre à votre compte.
- Vérifiez que l'identifiant du compte est autorisé pour consulter l'offre privée. Certains éditeurs de logiciels indépendants utilisent des listes limitées. Demandez à l'ISV s'il a autorisé votre compte à accéder au produit. L'autorisation de mise en vente est nécessaire pour les offres limitées de produits AMI. Si vous faites partie d'une AWS organisation et que le vendeur étend l'offre au compte de gestion, les comptes associés doivent être autorisés à s'abonner. Dans le cas contraire, les comptes associés de l'acheteur qui ne sont pas autorisés recevront le message d'erreur « Page introuvable » (404) lorsqu'il tentera de consulter l'offre.
- Vérifiez auprès de votre AWS administrateur que vous disposez des autorisations `aws-marketplace:ViewSubscriptions` IAM si vous devez consulter l'offre. Pour plus d'informations sur AWS Marketplace la sécurité, consultezSécurité sur AWS Marketplace.
- Vérifiez si vous utilisez une place de marché privée.
  - Assurez-vous que le produit figure sur la liste des produits autorisés de votre site de vente privé (le cas échéant), afin de pouvoir l'acheter. En cas de doute, contactez votre administrateur système pour vérifier.

Aucune de ces suggestions ne fonctionne

Si aucune des suggestions précédentes n'a résolu l'erreur 404 (Not Found) du code d'état HTTP, essayez les actions suivantes dans votre navigateur :

- Videz le cache.
- Supprimez les cookies.
- Déconnectez-vous, puis reconnectez-vous.
- Utilisez un mode de navigation privée ou privée.
- Essayez un autre navigateur. Nous vous déconseillons d'utiliserInternet Explorer.

Si vous avez suivi toutes les suggestions de résolution des problèmes et que vous recevez toujours le message d'erreur « Page introuvable », envoyez un e-mail à <mpcustdesk@amazon.com> pour obtenir de l'aide.

Page d'offres privées dans AWS Marketplace

DansAWS Marketplace, la page Offres privées répertorie toutes les offres privées qui vous ont été proposées Compte AWS pour des produits privés et publics. Toutes les offres mises à votre disposition sont affichées pour chaque produit. Vous pouvez accepter une offre pour chaque produit.

Comprendre la page des offres privées

Vous pouvez consulter la page de vos offres privées en vous connectant à la AWS Marketplace console et en accédant aux offres privées. Les offres privées qui vous sont proposées Compte AWS sont répertoriées sous Offres privées, y compris le numéro de l'offre, le produit, le vendeur officiel (ISV ou partenaire de distribution), l'éditeur, les contrats actifs (le cas échéant) et la date d'expiration de l'offre. Vous pouvez sélectionner le numéro d'offre correspondant à l'offre qui vous intéresse pour consulter les détails de l'offre et souscrire à une offre privée.

La page des offres privées contient les informations suivantes :

- L'onglet Offres disponibles répertorie les offres privées étendues à votre compte qui peuvent être acceptées. Le lien vers le numéro de l'offre sur cet onglet est le même que celui que le vendeur vous a peut-être fourni pour accéder aux détails de l'offre privée.
- L'onglet Offres acceptées et expirées répertorie les offres que vous avez acceptées et qui ont donné lieu à la création d'un accord. Il répertorie également les offres qui ont atteint la date d'expiration fixée par le vendeur. Cet onglet peut être utile pour récupérer un numéro d'offre et un numéro d'accord antérieurs (s'ils sont disponibles) lors du renouvellement auprès d'un vendeur. Si l'offre a donné lieu à un accord et que le contrat est actif, vous pouvez choisir le contrat pour afficher la page détaillée de l'abonnement.

> **Note**
>
> Les offres privées à date future sont répertoriées comme des renouvellements anticipés. Pour plus d'informations, consultez the section called “Travailler avec de futurs accords datés”.

Pour plus d'informations sur la modification, la mise à niveau ou le renouvellement d'une offre privée, consultezModification de l’abonnement à une offre privée ou désabonnement.

Autorisations requises pour consulter la page des offres privées

Pour consulter la page des offres privées dans la AWS Marketplace console, vous devez disposer des autorisations suivantes :

- Si vous utilisez des politiques AWS gérées : `AWSMarketplaceRead-onlyAWSMarketplaceManageSubscriptions`, ou `AWSMarketplaceFullAccess`
- Si vous n'utilisez pas de politiques AWS gérées : action `aws-marketplace:ListPrivateListings` IAM et `aws-marketplace:ViewSubscriptions`

Si vous ne parvenez pas à consulter la page des offres privées, contactez votre administrateur pour configurer les autorisations AWS Identity and Access Management (IAM) appropriées. Pour plus d'informations sur les autorisations IAM nécessaires pourAWS Marketplace, consultezAWSpolitiques gérées pour les AWS Marketplace acheteurs.

Abonnement à une offre privée SaaS

Pour une offre privée de logiciel en tant que service (SaaS), les options de configuration disponibles dépendent du contrat que vous êtes susceptible de négocier avec le vendeur.

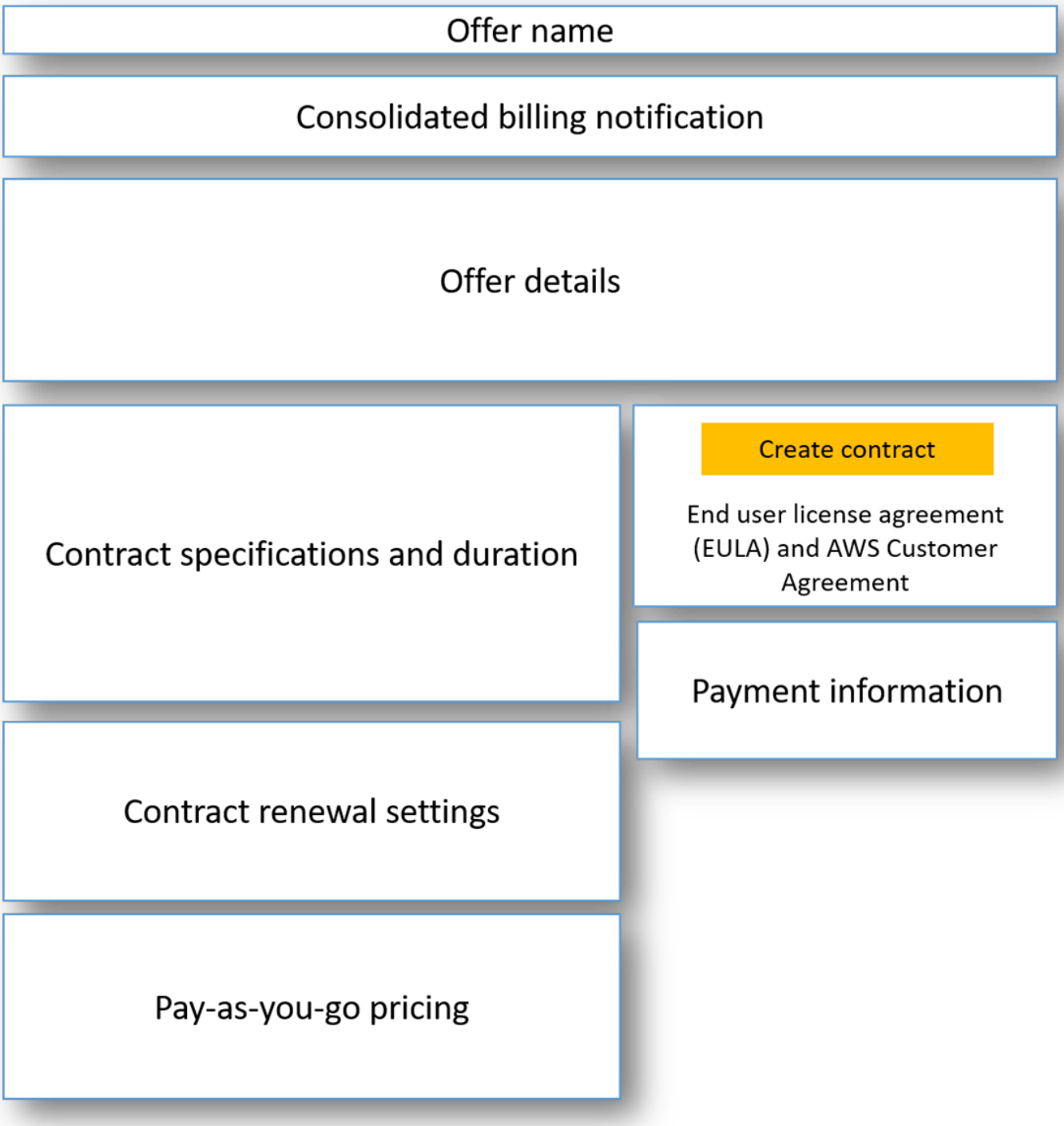
Comme le montre le schéma suivant, la page de l'offre privée comprend les sections suivantes :

- Nom de l'offre : il s'agit du nom que le vendeur a donné à votre offre privée lorsqu'il l'a créée.
- Informations de facturation consolidées — Cette notification apparaît si vous utilisez la facturation consolidée avec votreComptes AWS.
- Spécifications et durée du contrat — Ce volet indique la durée de l'offre et les dimensions qui la définissent. Les dimensions correspondent aux méthodes de mesure de l'utilisation et la durée pendant laquelle la tarification négociée reste en vigueur. Exemple : 5 Go/jour pendant 12 mois ou 0,01 USD par utilisateur et par heure. Si c’est un contrat qui fait l’objet de l'offre privée, vous payez pour une quantité d’utilisation convenue sur la durée du contrat. Si c’est un abonnement qui fait l’objet de l'offre privée, vous payez pour votre utilisation effective au tarif convenu.

> **Note**
>
> Les offres privées à date future sont répertoriées dans la catégorie des renouvellements anticipés. Pour plus d'informations, consultez the section called “Travailler avec de futurs accords datés”.

- Paramètres de renouvellement du contrat — Vous ne pouvez pas configurer les offres privées pour qu'elles soient renouvelées automatiquement. Pour les offres privées sur des produits SaaS, ce volet indique toujours qu’aucun renouvellement n’est disponible pour cette offre.
- ay-as-you-go Tarification P — Si vous négociez des prix pour l'utilisation du produit au-delà de ce qui est défini dans votre offre privée, les spécifications relatives au montant des coûts d'utilisation supplémentaires apparaissent ici. Par exemple, si vous avez conclu un contrat SaaS pour le stockage de données équivalent à 5 Go/jour pendant 12 mois et que vous utilisez 10 Go/jour, les 5 premiers Go sont inclus dans le contrat. Les 5 Go supplémentaires par jour sont facturés au prix indiqué. pay-as-you-go Avec les abonnements SaaS, un tarif est convenu quelle que soit la quantité utilisée pendant la durée du contrat.
- Contrat de licence utilisateur final (EULA) et bouton de création de contrat : c'est ici que vous pouvez consulter le contrat de licence que le vendeur a téléchargé pour cette offre privée. C’est également ici que vous pouvez accepter le contrat après vérification des spécifications de l’offre privée, lorsque vous êtes prêt à conclure le contrat.
- Informations de paiement — Ce volet décrit le moment où le paiement est dû et, si vous avez négocié un calendrier de paiement, la date et l'heure auxquelles le paiement est dû.

> **Important**
>
> Si une section n'apparaît pas sur la page de l'offre privée, cela signifie qu'il ne s'agit pas d'une partie négociée de l'offre privée.



Pour souscrire à une offre privée SaaS

1. Suivez les étapes pourAffichage d'une offre privée et abonnement.

2. Dans le volet des détails de l'offre, vérifiez que vous avez choisi la bonne offre privée. Il se peut que plusieurs offres s'affichent pour un même produit.
3. Dans le volet des spécifications et de la durée du contrat, vérifiez que la durée et les détails du contrat correspondent à ce que vous avez négocié. Si ce n'est pas le cas, vérifiez que vous avez sélectionné l'offre privée adéquate ou contactez le vendeur qui a créé l'offre.

> **Note**
>
> Les offres privées à date future sont répertoriées dans la catégorie des renouvellements anticipés. Pour plus d'informations, consultez the section called "Travailler avec de futurs accords datés".

4. Si vous avez négocié le pay-as-you-go prix, un volet contenant des informations décrivant les conditions négociées doit être affiché. Vérifiez les informations. Si certains éléments sont absents (et que vous vous y attendiez), contactez le vendeur.
5. Dans le volet des informations de paiement, vérifiez que tout est en ordre. Si vous avez négocié un calendrier de paiement flexible, les dates des paiements et les montants sont indiqués. Si ce n'est pas le cas, la totalité du contrat est facturée lorsque vous acceptez l'offre.
6. Dans le volet du CLUF et de la création du contrat, vérifiez que le CLUF est bien celui que vous avez négocié avec le vendeur. Une fois que vous avez passé en revue l'ensemble des conditions générales du contrat, choisissez Create contract (Créer le contrat) pour accepter l'offre.

Une fois que vous avez accepté l'offre, une page de confirmation s'ouvre, indiquant que vous vous êtes abonné au produit avec succès. Choisissez Set Up Your Account (Configurer votre compte) pour être redirigé vers la page du vendeur et terminer la configuration de votre compte sur son site Web.

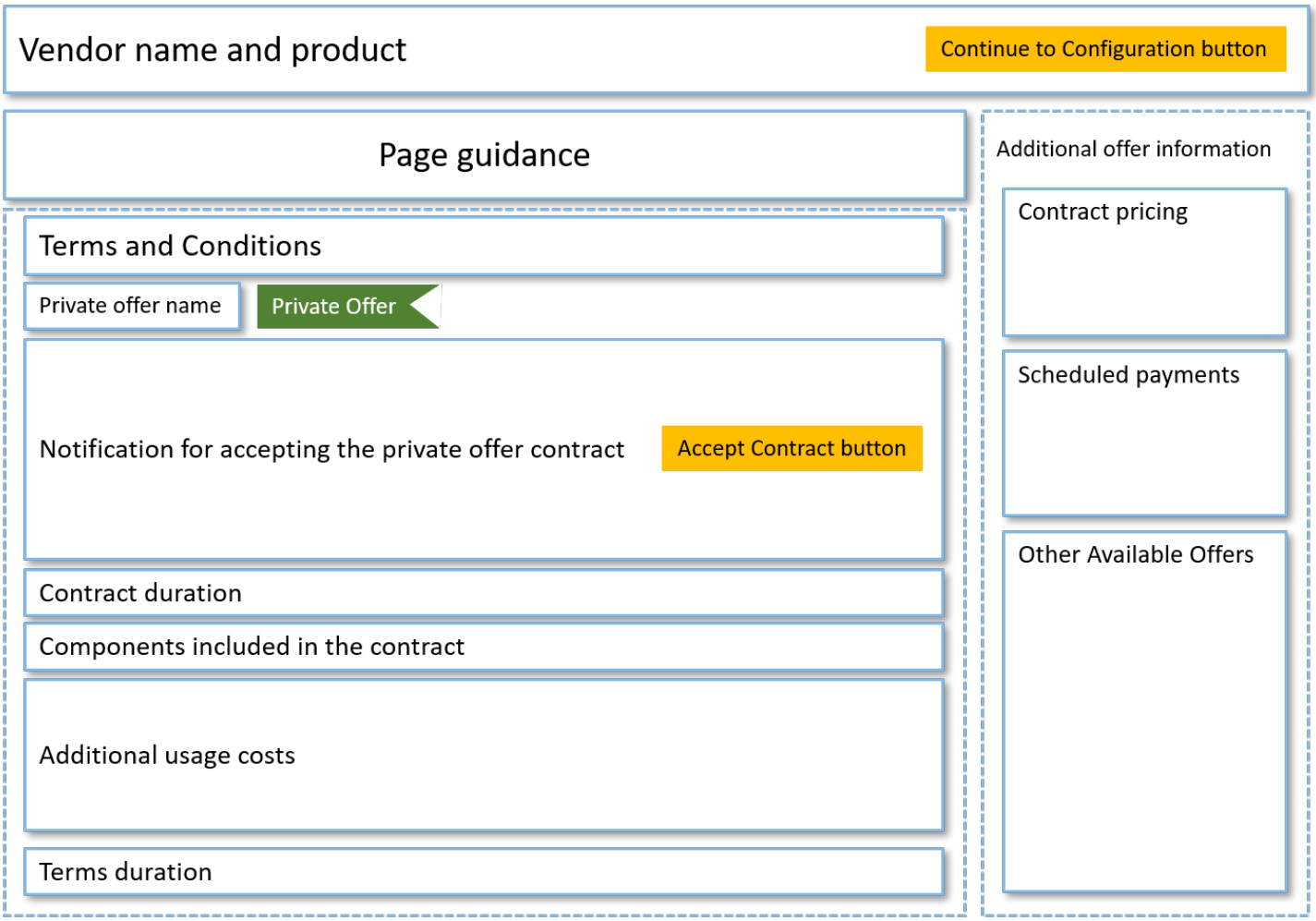
Abonnement à une offre privée AMI

Les sections et les options de configuration disponibles pour votre offre privée Amazon Machine Image (AMI) dépendent du contrat que vous négociez avec le fournisseur du produit. L'image suivante montre la mise en page d'une page d'offre privée AMI sur leAWS Marketplace site Web.

Comme le montre le diagramme suivant, la page de l'offre privée comprend les sections suivantes :

- Nom du fournisseur et produit : il s'agit du nom du fournisseur et du produit pour lequel l'offre privée est destinée. À droite se trouve le bouton de configuration du produit.

- Guide de page : cette zone contient des instructions pour effectuer les tâches de la page et accepter l'offre privée.
- Termes et conditions — Cette section comprend les informations suivantes :
  - En haut à gauche se trouvent le nom de l'offre privée et une étiquette indiquant qu'il s'agit d'une offre privée.
  - Sous la section du nom de l'offre privée se trouve une notification d'acceptation du contrat. Vous pouvez utiliser le bouton Accepter le contrat pour accepter l'offre privée.
  - Sous la section de notification se trouvent des sections relatives à la durée du contrat, aux composants inclus dans le contrat et à la tarification des instances que vous avez négociée, ainsi qu'une autre possibilité de consulter ou de télécharger le CLUF.
- Durée des termes — Cette section indique le nombre de jours du contrat et la date de fin du contrat.
- Informations supplémentaires sur l'offre — Sur la droite se trouvent des images miniatures du prix total du contrat, de votre prochain paiement prévu, des conditions actuelles et des autres offres privées et publiques disponibles.



Souscription à une offre privée AMI annuelle avec un calendrier de paiement flexible

Pour souscrire à une offre privée AMI, vous devez accepter l'offre privée sur leAWS Marketplace site Web. Vous ne pouvez pas accepter l'offre privée sur laAWS Marketplace console Amazon Elastic Compute Cloud (Amazon EC2). Si le vendeur crée une offre privée avec un calendrier de paiement flexible, les dates du calendrier de paiement vous sont facturées aux montants indiqués dans l'offre privée. Pour accepter une offre privée AMI avec un calendrier de paiement flexible, suivez la procédure suivante.

Pour accepter une offre privée AMI avec un calendrier de paiement flexible

1. Suivez les étapes pourAffichage d’une offre privée et abonnement.

2. Assurez-vous de consulter l’offre privée adéquate. Le fournisseur peut vous créer plusieurs offres privées pour son produit. Toutes les offres privées supplémentaires apparaissent dans la section Autres offres disponibles.
3. Vérifiez que la date d'expiration et les informations de tarification correspondent à ce que vous avez négocié dans le cadre de l’offre privée. Si ce n'est pas le cas, vérifiez que vous consultez l’offre privée adéquate.
4. Téléchargez le CLUF et vérifiez qu'il s'agit bien de ce que vous avez négocié pour l'offre privée.
5. Dans la section Durée des conditions, vérifiez que les conditions de l'offre privée correspondent à celles que vous avez négociées.
6. Après avoir vérifié les détails de l'offre privée, dans la section Termes et conditions, choisissez Accepter le contrat.
7. Passez en revue les conditions et choisissez Confirmer si vous les acceptez.

> **Important**
>
> Ne rafraîchissez pas votre navigateur pendant que le système traite la demande de votre contrat.

Lorsque vous êtes prêt à configurer l'AMI, choisissez Continue to Configuration (Passer à la configuration). La procédure d'abonnement est obligatoire pour chaque utilisation du produit.

Souscription à une offre privée AMI annuelle sans calendrier de paiement flexible

Pour souscrire à une offre privée AMI, vous devez accepter l'offre privée sur leAWS Marketplace site Web. Vous ne pouvez pas l'accepter sur laAWS Marketplace console Amazon EC2. Si le vendeur crée une offre privée sans calendrier de paiement flexible, vous pouvez configurer le contrat au moment de l'acceptation en fonction du prix et des options définis dans l'offre privée. Pour accepter une offre privée AMI sans calendrier de paiement flexible, suivez la procédure suivante.

Accepter une offre privée AMI sans calendrier de paiement flexible

1. Assurez-vous de consulter l’offre privée adéquate. Le fournisseur peut vous créer plusieurs offres privées pour son produit. Toutes les offres privées supplémentaires apparaissent dans le volet prévu à cet effet. Vérifiez que l'offre que vous souhaitez accepter apparaît sous la mention Afficher cette offre.

> **Note**
>
> Bien souvent, le compte payeur n’est pas le même que celui qui utilise le produit. Nous vous recommandons de lancer le produit manuellement au lieu de choisir l'option 1-Click si vous acceptez l'offre via le compte payeur.

2. Vérifiez que la date d'expiration et les informations de tarification correspondent à ce que vous avez négocié dans le cadre de l’offre privée. Si ce n'est pas le cas, vérifiez que vous consultez l’offre privée adéquate.
3. Téléchargez le CLUF et vérifiez qu'il s'agit bien de ce que vous avez négocié pour l'offre privée.
4. Dans le volet des clauses du contrat, vérifiez que les conditions générales correspondent à ce que vous avez négocié dans le cadre de l’offre privée.
5. Vérifiez si les détails de l'offre correspondent à ce que vous avez négocié pour l'offre privée, puis choisissez Accept Terms (Accepter les conditions). Si ce n'est pas le cas, vérifiez que vous consultez l’offre privée adéquate.
6. Pour S'abonner à ce logiciel, sélectionnez Type d'instance dans la liste des types d'instance disponibles. Dans Quantité, choisissez le nombre de licences.
7. Vérifiez vos sélections. Lorsque vous êtes satisfait, choisissez Créer un contrat, puis cliquez sur Confirmer.

Lorsque vous êtes prêt à configurer l'AMI, choisissez Continue to Configuration (Passer à la configuration). La procédure d'abonnement est obligatoire pour chaque utilisation du produit.

Modification de l’abonnement à une offre privée ou désabonnement

Vous pouvez passer d'abonnements standard à des offres privées, et vous pouvez également modifier certaines offres privées existantes dansAWS Marketplace. Le processus dépend de l'accord que vous avez conclu.

Pour de nombreux abonnements, lorsque vous passez d’une tarification publique à une offre privée, vous négociez l'offre avec le FIL ou votre partenaire de distribution. Dès que vous acceptez une offre privée, le ou les abonnements existants associés adoptent automatiquement le modèle de tarification de l’offre privée. Vous n’avez pas besoin d’intervenir. Lisez les instructions suivantes pour identifier le scénario qui s’applique à vous et les étapes à suivre pour bénéficier de la tarification de l’offre privée.

Passage de la tarification d’une offre publique à une offre privée

Une fois que vous avez accepté l'offre privée, aucune autre action n'est nécessaire pour l'utilisateur qui a accepté l'offre. La tarification et les conditions générales définies dans l’offre privée sont directement appliquées. Pour passer aux prix, aux termes et conditions de l'offre privée, chaque utilisateur lié utilisant le produit doit accepter l'offre privée. Tout utilisateur qui commence à utiliser le produit doit également accepter l'offre privée pour obtenir les prix, les termes et conditions définis dans l'offre privée.

Modification d'un contrat SaaS : mises à niveau et renouvellements

Cette section s'applique au contrat de logiciel en tant que service (SaaS) et au contrat SaaS avec des produits de consommation. Si vous avez un contrat actif issu d'une offre privée précédente et que vous souhaitez accepter une nouvelle offre privée pour le même produit, le vendeur peut mettre à niveau ou renouveler votre contrat existant pour en modifier les termes, le prix ou la durée, ou pour renouveler votre contrat existant avant son expiration. Cela se traduira par une nouvelle offre privée que vous pourrez accepter, sans avoir à annuler au préalable votre contrat existant.

> **Note**
>
> Les offres privées à date future sont répertoriées dans la catégorie des renouvellements anticipés. Pour plus d'informations, consultez the section called “Travailler avec de futurs accords datés”.

Pour accepter une mise à niveau ou un renouvellement, vous devez respecter les conditions de facturation. Si vous n'êtes pas actuellement soumis aux conditions de facturation, envoyez un ticket au service AWS client pour remplacer votre mode de paiement par la facturation.

Si vous ne souhaitez pas passer à la facturation, vous pouvez effectuer l'une des actions suivantes :

- Travaillez avec le fournisseur du produit et l'équipe de support AWS Marketplace client pour annuler le contrat en cours avant d'accepter une nouvelle offre privée pour ce produit
- Acceptez l'offre sur un autreCompte AWS.

Passage d'un abonnement SaaS à un contrat SaaS

Pour passer d'un abonnement SaaS à un contrat SaaS, vous devez d'abord vous désabonner de l'abonnement SaaS. Ensuite, vous devez accepter l'offre privée pour le contrat SaaS. Pour consulter vos abonnements SaaS existants, choisissez Your Marketplace Software dans le coin supérieur droit de la AWS Marketplace console.

Passage d'un contrat AMI à un nouveau contrat

Si vous avez conclu un contrat Amazon Machine Image (AMI) issu d'une offre privée précédente et que vous souhaitez accepter une nouvelle offre privée pour le même produit, vous devez effectuer l'une des opérations suivantes :

- Attendez que le contrat AMI actuel expire avant d'accepter le nouveau contrat AMI.
- Travaillez avec le fournisseur du produit et l'équipe du support AWS Marketplace client pour résilier votre contrat actuel.
- Acceptez l'offre privée en utilisant une offre Compte AWS différente de celle qui contient le contrat

Passage d'un abonnement AMI horaires à un abonnement AMI annuelles

Lorsque vous passez d'un abonnement AMI horaires à un abonnement AMI annuelles, c'est un système de bon qui est mis en place. Chaque heure d'utilisation AMI est compensée par une unité dans l'abonnement annuel AMI. Lorsque vous achetez l'abonnement annuel via une offre privée, tous les comptes associés abonnés au produit passent automatiquement à la tarification négociée dans l'offre privée. Les comptes associés qui entament un abonnement après la mise en place de l'offre privée doivent s'abonner à l'offre privée.

> **Note**
>
> Les licences annuelles de votre ancienne offre sont désactivées dès l'acceptation des conditions de la nouvelle offre. Consultez le FIL pour discuter de la rémunération des anciennes licences et de la façon de poursuivre avec la nouvelle offre.

Passage d’un abonnement AMI annuelles à un abonnement AMI horaires

Lorsque votre abonnement annuel expire, tous les comptes associés abonnés au produit basculent automatiquement vers une tarification AMI à l’heure. En cas d’abonnement annuel, le compte associé ne peut pas bénéficier d’un abonnement horaire pour ce produit sans annuler l'abonnement.

Travailler avec de futurs contrats datés et des offres privées

Avec les contrats à date future (FDA) en vigueurAWS Marketplace, vous pouvez vous abonner à des produits dont l'utilisation commence à une date ultérieure. Vous pouvez gérer le moment où vous achetez un produit indépendamment du moment où vous le payez et du moment où vous l'utilisez.

La FDA aide les acheteurs à effectuer les actions suivantes de manière indépendante pour les transactions sur AWS Marketplace :

- Procurez-vous le produit/réservez l'offre en acceptant l'offre.
- Commencez à utiliser le produit (activation de la licence/des droits).
- Payer un achat (génération de factures).

La FDA est soutenue sur des offres privées, en créant des produits pour les logiciels en tant que service (SaaS), pour les contrats et les contrats avec tarification à la consommation (CCP), et avec ou sans paiements flexibles.

Lorsque vous utilisez des contrats à date future, gardez à l'esprit les dates suivantes :

Date de signature de l'accord

: Date à laquelle vous avez accepté l'offre et date à laquelle le contrat a été créé. C'est à cette date que l'identifiant de l'accord est créé.

Date de début de l'accord

: Date à laquelle l'utilisation de votre produit commence. Il s'agit de la date future ou de la future date de début. Il s'agit de la date à laquelle votre licence ou votre droit est activé.

Date de fin de l'accord

: Date à laquelle le contrat prend fin. Le contrat et la licence/le droit expirent à cette date.

Pour plus d'informations sur l'utilisation des FDA, consultez les rubriques suivantes :

Rubriques

Création de futurs accords datés

Pour les contrats SaaS et les contrats avec tarification à la consommation, avec ou sans calendrier de paiement flexible, le vendeur définit la date de début du contrat dans le cadre de la génération d'une offre privée. En tant qu'acheteur, vous devez travailler avec les vendeurs pour vous assurer que la date de début répond à vos exigences.

Pour créer un futur accord daté, suivez la procédure ci-dessous. Vous pouvez consulter vos futurs contrats dans la AWS Marketplace console sur la page Gestion des abonnements.

Pour créer un futur accord daté

1. Suivez les étapes pourAffichage d’une offre privée et abonnement.
2. Dans le volet des détails de l'offre, vérifiez que vous avez choisi la bonne offre privée et que la date de début du contrat est correcte. Les offres à date future sont marquées comme des renouvellements anticipés dans le menu déroulant des offres.

> **Note**
>
> Pour les produits SaaS, à la date de début du contrat, vous devez vous assurer d'avoir terminé la configuration de votre compte auprès de l'ISV. Vous ne pouvez pas effectuer cette étape avant la date de début de l'accord. Pour plus d’informations, consultez the section called “Abonnement à une offre privée SaaS”.

Utilisation d'un planificateur de paiement flexible avec des accords futurs

Vous pouvez utiliser le planificateur de paiement flexible pour les contrats futurs. Vous pouvez configurer le paiement des achats à l'heure de votre choix entre la date de signature de votre contrat et la date de fin du contrat. Cette approche inclut les paiements avant et après la date de début de l'accord.

Le vendeur officiel qui crée l'offre privée choisit les dates et les montants des paiements. Pour plus de détails, consultez la section Planificateur de paiement flexible.

Modification de vos futurs contrats

Vous pouvez augmenter le nombre d'unités achetées d'une certaine dimension auprès de votre FDA avant et après la date de début de l'accord. Cette option est possible lorsque l'accord ne prévoit pas de calendrier de paiement flexible. Pour plus de détails, consultez la section Planificateur de paiement flexible.

Le montant calculé au prorata vous sera facturé à la date de début du contrat lorsque votre modification sera terminée. Si votre date de début est passée, vous serez débité immédiatement.

Réception de notifications concernant de futurs accords datés

Vous recevez des notifications par e-mail envoyées à votre compte root désigné concernant les mesures suivantes prises dans le cadre de vos futurs contrats :

- Acceptation de l'offre/création du contrat (date de signature du contrat)
- Lors de l'activation de la licence ou des droits (date de début du contrat)
- Rappels pour les accords expirant 30, 60 ou 90 jours à l'avance
- Expiration du contrat (date de fin du contrat)
- Lors d'une modification ou d'un remplacement du contrat

Partage d'abonnements au sein d'une organisation

Lorsque vous vous abonnez à des produits enAWS Marketplace, un contrat est créé qui vous accorde une licence d'utilisation de ces produits. Si vousCompte AWS êtes membre d'une organisation, vous pouvez partager cette licence pour Amazon Machine Image (AMI), le conteneur, l'apprentissage automatique et les produits de données avec les autres comptes de cette organisation. Vous devez configurer la prise en charge des licences dansAWS Marketplace, puis la partager depuis l'intérieurAWS License Manager.

> **Note**
>
> Pour plus d'informations sur AWS Organizations, consultez le AWS OrganizationsGuide de l'utilisateur .
> Pour plus d'informations sur le partage de licences avec votre organisation dansAWS License Manager, consultez la section Licences accordées dans le Guide deAWS License Manager l'utilisateur.

La vidéo suivante constitue une présentation de l'expérience de partage de licence.

Distribuez vos droits deAWS Marketplace licence (3:56)

Les rubriques suivantes décrivent le processus d'affichage, de partage et de suivi des licences entre comptes.

Rubriques

- Prérequis pour le partage de licence
- Affichage de vos licences
- Partage de vos licences
- Suivi de l'usage des licences

Prérequis pour le partage de licence

Avant de pouvoir partager des licences,AWS Marketplace vous devez configurer le partage de licences pour votre organisation. Exécutez les tâches suivantes pour configurer le partage de licences pour votre organisation :

- AWS MarketplaceAutorisez la société à gérer les licences en votre nom afin qu'elle puisse créer les licences associées lorsque vous achetez ou partagez vos licences. Pour plus d'informations, veuillez consulter Utiliser des rôles pour partager des droits pour AWS Marketplace.
- ConfigurezAWS License Manager pour la première utilisation. Pour plus d'informations, consultez la section MiseAWS License Manager en route du Guide deAWS License Manager l'utilisateur.

Affichage de vos licences

AWS Marketplacecrée automatiquement des licences pour les AMI, les conteneurs, l'apprentissage automatique, les logiciels en tant que service (SaaS) et les produits de données que vous achetez. Vous pouvez partager ces licences avec d'autres comptes de votre organisation.

> **Note**
>
> Bien que des licences soient créées pour les produits SaaS, le partage de licences SaaS n'est actuellement pas pris en charge.

Vous gérez et partagez des licences à l'aide deAWS License Manager. Toutefois, vous pouvez l'utiliserAWS Marketplace pour consulter les licences des produits que vous avez achetés directementAWS Marketplace.

Pour consulter les licences des produits auxquels vous êtes abonné dansAWS Marketplace

1. Connectez-vous AWS Marketplace, puis choisissez Gérer les abonnements.
2. Vous pouvez consulter toutes les licences ou consulter la licence d'un abonnement spécifique.
    - Pour afficher toutes les licences
        - Dans le menu Actions, sélectionnez Afficher les licences pour afficher toutes les licencesAWS Marketplace gérées dans la console License Manager.
    - Pour afficher les licences d'un abonnement unique
        a. Choisissez la fiche du produit que vous souhaitez visualiser pour accéder à sa page de détails du produit.
        b. Dans le menu Actions, sélectionnez Afficher la licence pour afficher la licence de ce produit dans la console License Manager.

> **Note**
>
> Vous pouvez également consulter les licences accordées qui ont été agrégées à partir de tous les comptes de votre organisation. Pour plus d'informations, veuillez consulter la rubrique Licences accordées dans le Guide de l'utilisateur AWS License Manager.

Partage de vos licences

Seuls les produits AMI, les conteneurs, l'apprentissage automatique et les produits de données disposent de licences pouvant être partagées.

Les abonnementsAWS Marketplace ont un niveau d'accès indiqué dans les détails du produit :

- Les produits dotés d'un niveau d'accord disposent d'une licence que vous pouvez utiliser et partager avec d'autres comptes de votre organisation.
- Les produits dotés d'un niveau d'autorisation sont des licences qui ont été partagées avec votre compte. Vous pouvez utiliser ces produits, mais vous ne pouvez pas les partager.

AWS Marketplaceprend en charge les subventions, qui partagent l'utilisation d'une licence directement avecAWS OrganizationsCompte AWS, ou une unité organisationnelle utilisantAWS License Manager. Le processus d'activation des subventions inclut désormais des options supplémentaires pour remplacer les subventions activées pour le même produit d'origineAWS Marketplace. Pour plus d'informations, veuillez consulter la rubrique Licences accordées dans le Guide de l'utilisateur AWS License Manager.

> **Note**
>
> Pour les produits limités à certains produitsRégions AWS, un compte avec lequel vous partagez votre licence ne peut activer la licence que si le compte se trouve dans une région autorisée.

Suivi de l'usage des licences

Vous pouvez suivre vos statistiques de licence basées sur l'utilisation pour les produits AMI enAWS License Manager sélectionnant l'onglet Tableau de bord d'utilisation dans chaque licence respective.

Pour plus d'informations sur l'utilisation du License Manager pour suivre l'utilisation de vos licences, consultez la section Licences accordées dans le Guide deAWS License Manager l'utilisateur.

Notifications aux acheteurs concernant les AWS Marketplace événements

AWS Marketplacefournit des notifications en temps opportun par e-mail, via Amazon EventBridge Events et via les rubriques Amazon Simple Notification Service (Amazon SNS).

Rubriques

- Notifications par e-mail pour les AWS Marketplace événements
- EventBridge Notifications Amazon pour les AWS Marketplace événements

Notifications par e-mail pour les AWS Marketplace événements

En tant qu'acheteurAWS Marketplace, vous recevez une notification par e-mail lorsque l'une des situations suivantes se produit :

- Vous acceptez une offre.
- Un vendeur publie une nouvelle offre privée liée à l'offre privée que vous avez acceptée précédemment ou publie une mise à jour de l'offre précédemment acceptée.

> **Note**
>
> Les notifications sont envoyées à l'adresse e-mail associée à l'Compte AWSidentifiant acheteur.

EventBridge Notifications Amazon pour les AWS Marketplace événements

AWS Marketplaceest intégré à Amazon EventBridge, anciennement appelé Amazon CloudWatch Events. EventBridge est un service de bus d'événements que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

En tant qu'acheteur, vous recevez un événement AWS Marketplace chaque fois qu'un vendeur crée une offre et la met en vente. L'événement contient des informations telles que l'identifiant, la date d'expiration, les détails du produit et le nom du vendeur.

Rubriques

AWS Marketplace EventBridge Événements Amazon de l'API Discovery

Cette rubrique fournit des informations détaillées sur chaque événement répertorié dans le tableau suivant.

Action du vendeur	Événement reçu par l'acheteur	Rubrique connexe
Crée une offre et la rend disponible à l'achat	`Listing Available`	the section called “Événements pour les nouvelles annonces”

Événements pour les nouvelles annonces

Lorsqu'un vendeur crée une offre et la met en vente, l'acheteur reçoit un événement avec le type de détail suivant :`Listing Available`.

> **Note**
>
> Pour plus d'informations sur la création de EventBridge règles, consultez EventBridge les règles Amazon dans le guide de EventBridge l'utilisateur Amazon.

Voici un exemple de corps d'événement pour un `Listing Available` événement.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "Listing Available",
    "source": "aws.discovery-marketplace",
    "account": "123456789012",
    "time": "2023-08-26T00:00:00Z",
```

```
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "requestId": "3d4c9f9b-b809-4f5e-9fac-a9ae98b05cbb",
        "catalog": "AWSMarketplace",
        "offer": {
            "id": "offer-1234567890123",
            "expirationDate": "2025-08-26T00:00:00Z"
        },
        "product": {
            "id": "bbbbaaaa-abcd-1111-abcd-666666666666",
            "title": "Product Title"
        },
        "sellerOfRecord": {
            "name": "Seller Name"
        }
    }
}
```

Intégration de AWS Marketplace à des systèmes d'approvisionnement

Vous pouvez configurer l'intégration AWS Marketplace et votre logiciel d'approvisionnement Coupa ou SAP Ariba. Une fois que vous avez terminé la configuration, les utilisateurs de votre organisation peuvent utiliser votre logiciel d'approvisionnement pour rechercher des produits AWS Marketplace et demander de s'abonner à ceux-ci. Une fois que la demande d'abonnement est approuvée, la transaction est terminée, et l'utilisateur est averti que son abonnement au logiciel est disponible. Lorsque l'utilisateur se connecte à AWS Marketplace, le produit logiciel est répertorié en tant qu'abonnement acheté et est disponible pour utilisation. L'intégration à votre système d'approvisionnement permet également d'intégrer vos AWS Marketplace factures à votre système de bons de commande.

Comment fonctionne l'intégration des achats

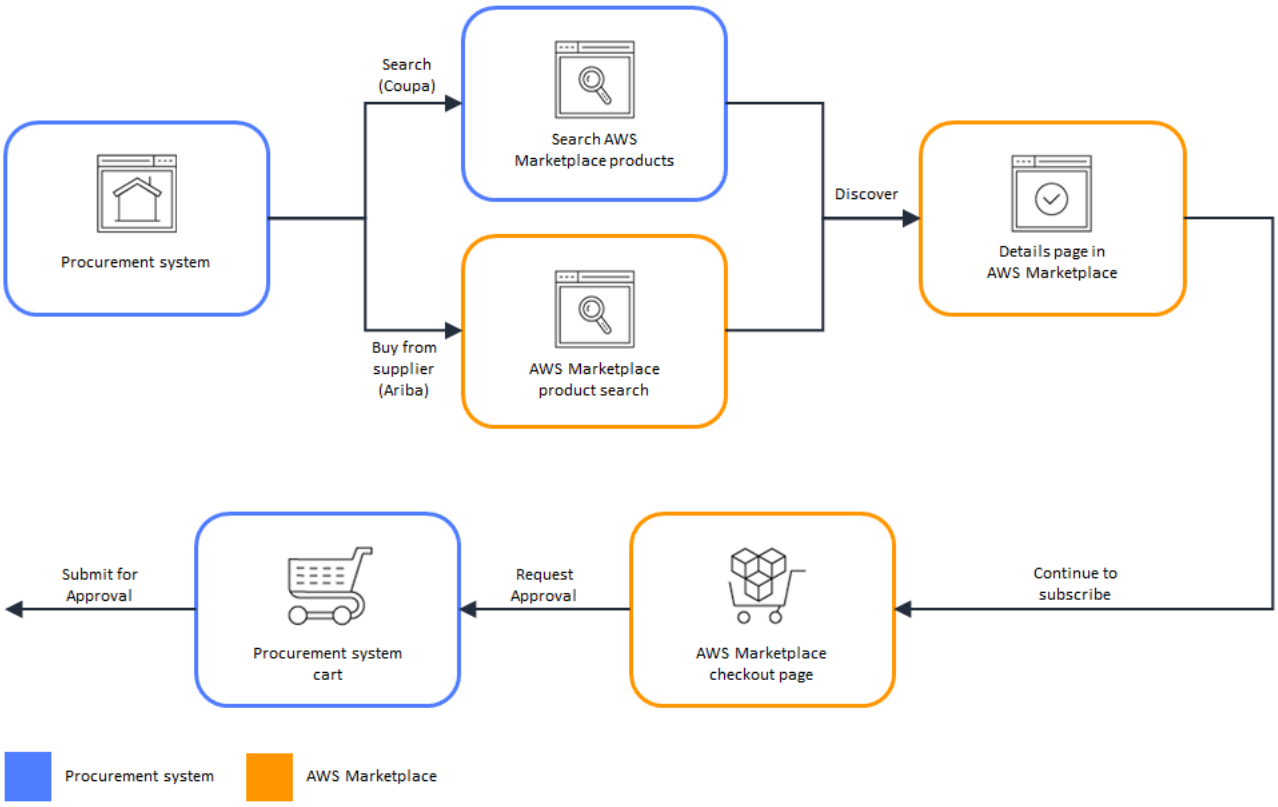
Vous pouvez configurer le logiciel d'approvisionnement pour qu'il s'intègre AWS Marketplace au protocole cXML (Commerce Extensible Markup Language). Cette intégration crée un point d'accès au catalogue d'un tiers, appelé punchout.

L'intégration diffère légèrement en fonction du système d'approvisionnement :

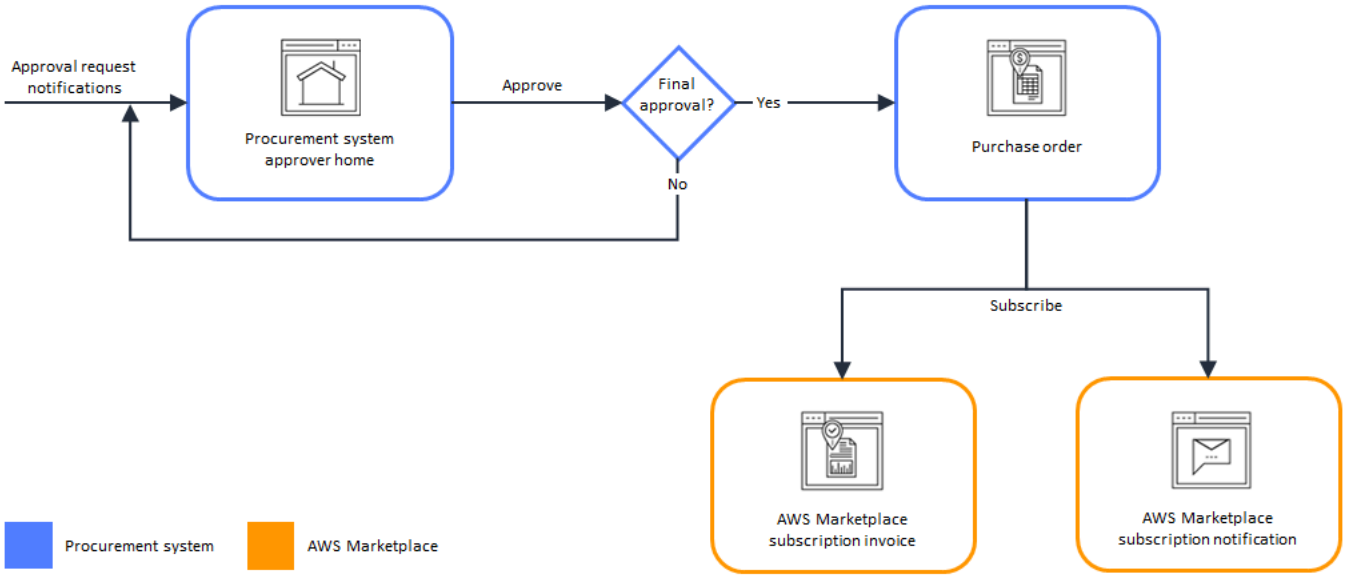
- Coupa : à l'aide de la fonction Coupa Open Buy, vous pouvez effectuer une recherche AWS Marketplace depuis Coupa. Coupa affiche les résultats de recherche et, lorsque l'utilisateur choisit un produit, il est redirigé AWS Marketplace vers celui-ci pour en voir les détails. Les utilisateurs du logiciel d'approvisionnement de Coupa peuvent également accéder au AWS Marketplace catalogue dans la section Shop Online de leur page d'accueil. L'utilisateur peut également choisir de démarrer directement AWS Marketplace pour rechercher des produits.
- SAP Ariba — Ariba redirige les utilisateurs AWS Marketplace vers la recherche de logiciels et l'obtention de détails sur un produit. Une fois qu'un administrateur a configuré l'intégration Punchout, les utilisateurs du logiciel d'approvisionnement d'Ariba peuvent trouver des AWS Marketplace logiciels en cliquant sur l'onglet Catalogue, puis en sélectionnant le catalogue. AWS Marketplace Cela les redirige AWS Marketplace vers les produits qui les intéressent.

  Les utilisateurs d'Ariba doivent initier leur achat depuis Ariba, et non depuis Ariba. AWS Marketplace

Lorsque l'utilisateur souhaite acheter un abonnement dans lequel il navigueAWS Marketplace, il crée une demande d'abonnement dansAWS Marketplace. Sur la page d'abonnement du produit, au lieu de finaliser l'achat, l'utilisateur demande une approbation. La demande est renvoyée vers un panier d'achat dans le système d'approvisionnement pour terminer le processus d'approbation. Le schéma suivant montre le processus d'une demande d'abonnement au système d'approvisionnement.



Lorsque le système d'approvisionnement reçoit la demande deAWS Marketplace, il lance un flux de travail pour terminer le processus d'approbation. Une fois la demande approuvée, le système de bons de commande du système d'approvisionnement termine automatiquement la transaction AWS Marketplace et informe l'utilisateur que son abonnement est prêt à être déployé. Le demandeur n'a pas besoin de revenir pour AWS Marketplace terminer l'achat. Toutefois, ils voudront peut-être y retourner AWS Marketplace pour obtenir des instructions sur la façon d'utiliser le produit qu'ils ont acheté. AWS Marketplaceenvoie un e-mail au AWS compte utilisé pour accéderAWS Marketplace. Le message électronique informe le destinataire que l'abonnement a réussi et que le logiciel est disponible viaAWS Marketplace. Le schéma suivant montre le processus d'approbation d'une demande d'abonnement au système d'approvisionnement.



Les remarques supplémentaires concernant l'intégration aux systèmes d'approvisionnement sont les suivantes :

- Les essais gratuits ne génèrent pas de facture dans le système d'approvisionnement, car aucun frais ne leur est associé.
- Les contrats qui comportent des frais uniques en plus des pay-as-you-go frais peuvent nécessiter deux séries d'approbations. L'une des approbations concerne le prix contractuel (ou annuel) et l'autre le prix horaire ou unitaire (pay-as-you-go).
- Les clients disposant de PSI (Procurement System Integrations) peuvent activer les pré-approbations pour les produits gratuits et les produits BYOL. Il existe deux paramètres, un pour Free et un pour BYOL. Lorsque le paramètre est activé, les commandes sont préapprouvées et les AWS Marketplace clients n'ont pas besoin de soumettre des commandes à leur système d'approvisionnement pour approbation. Lorsque le paramètre est désactivé, les clients soumettent des approbations via le bouton Demander une approbation à leur système d'approvisionnement. Lorsque le paramètre de pré-approbation pour les produits Free et BYOL est désactivé, les commandes de 0,00$ sont produites dans le système d'approvisionnement du client. Pour plus d'informations sur les intégrations des systèmes d'approvisionnement, voir https://aws.amazon.com/marketplace/features/procurementsystem

Configuration de l'intégration du système d'approvisionnement

Pour configurer l'intégration entre AWS Marketplace et votre système d'approvisionnement, vous devez démarrer le processus AWS Marketplace et le terminer dans le système d'approvisionnement. Vous utilisez les informations générées dans AWS Marketplace pour configurer le punchout du système d'approvisionnement. Pour que vous puissiez terminer la configuration, les comptes que vous utilisez doivent répondre aux exigences suivantes :

- Le compte de gestion doit être Compte AWS utilisé pour terminer la AWS Marketplace configuration et disposer des autorisations AWS Identity and Access Management (IAM) définies dans la politique `AWSMarketplaceProcurementSystemAdminFullAccess` gérée.
- Le compte du système d'approvisionnement utilisé pour terminer la configuration doit disposer d'un accès administratif pour configurer un contrat, un fournisseur et un catalogue détaillé dans le système d'approvisionnement.

Configuration des autorisations IAM

Les autorisations IAM suivantes figurent dans la politique AWSpolitique gérée : AWSMarketplaceProcurementSystemAdminFullAccess gérée et sont requises pour configurer l'intégration entre AWS Marketplace et un système d'approvisionnement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Nous vous recommandons d'utiliser les autorisations gérées par IAM plutôt que de les configurer manuellement. L'utilisation de cette approche est moins propice aux erreurs humaines et si les autorisations changent, la stratégie gérée est mise à jour. Pour plus d'informations sur la configuration et l'utilisation d'IAM dansAWS Marketplace, consultezSécurité sur AWS Marketplace.

Configuration AWS Marketplace pour l'intégration à Coupa

Une fois que vous avez configuré vos autorisations IAM, vous êtes prêt à configurer AWS Marketplace l'intégration avec Coupa. Accédez à Gérer les achats. Dans le volet Gérer les systèmes d'approvisionnement, entrez un nom et une description pour le poinchout. Vous pouvez également passer l'intégration en mode test afin que les utilisateurs puissent tester l'intégration sans créer d'abonnements aux produits jusqu'à ce que vous soyez prêt. Pour configurer la portion AWS Marketplace de l'intégration, effectuez la procédure suivante.

Pour configurer AWS Marketplace pour une intégration à Coupa

1. Dans AWS Marketplace Manage Procurement Systems (Gérer les systèmes d'approvisionnement), sous Procurement systems (Systèmes d'approvisionnement), choisissez Set up Coupa integration (Configurer l'intégration à Coupa).
2. Sur la page Manage Coupa integration (Gérer l'intégration à Coupa), sous Account information (Informations sur le compte), entrez le nom et la description de votre intégration.

   > **Note**
   >
   > Vous souhaiterez peut-être que vos factures affichées dans la AWS Billing console fassent référence au bon de commande cXML (Commerce Extensible Markup Language) utilisé pour souscrire à votre produit contractuel SaaS (logiciel en tant que service). Si tel est le cas, vous pouvez activer l'intégration de facturation à l'aide d'un rôle lié à un service dans les AWS Marketplace paramètres.

3. Vous pouvez activer ou désactiver les paramètres de configuration pour Activer la redirection et le mode Test, puis sélectionner Enregistrer pour terminer l'intégration dans le AWS Marketplace système.

Une fois que vous avez terminé l'intégration dansAWS Marketplace, vous devez procéder à la configuration de l'intégration dans Coupa. Vous utilisez les informations générées sur cette page pour configurer le punchout dans votre système Coupa.

La AWS Marketplace configuration indique par défaut que le mode test est activé. En mode test, les demandes d'abonnement sont envoyées au backend Coupa afin que vous puissiez voir le flux complet, mais aucune facture finale n'est créée. Cela vous aide à finaliser la configuration et à activer le punchout de façon planifiée.

> **Note**
>
> Vous pouvez activer ou désactiver le mode test, selon vos besoins.
> N'oubliez pas de désactiver le mode test lorsque vous avez terminé votre intégration. Dans le cas contraire, les utilisateurs de votre système sembleront créer des demandes, mais aucun logiciel ne sera acheté.

Configuration de Coupa

Pour configurer l'intégration avec AWS Marketplace votre système Coupa, copiez les informations du volet Informations sur les achats de la page Gérer l'intégration Coupa dans. AWS Marketplace Utilisez ces informations pour suivre les étapes décrites dans les liens suivants qui vous guideront dans la configuration de votre système d'approvisionnement Coupa :

- Configuration de Coupa Punchout
- Configuring a Supplier for cXML Purchase Orders

> **Note**
>
> Pour plus d'informations sur les codes UNSPSC utilisés parAWS Marketplace, reportez-vous à la section. Codes UNSPSC utilisés par AWS Marketplace

Configuration AWS Marketplace pour l'intégration à SAP Ariba

Pour configurer AWS Marketplace l'intégration à Ariba, vous devez travailler avec l'équipe des AWS Marketplace opérations afin de créer un poinçonnage de niveau 1. Pour plus d'informations sur SAP Ariba Punchout, consultez la section Présentation de SAP Ariba PunchOut sur le site Web de la communauté SAP.

Rassemblez les informations suivantes pour préparer la configuration de l'installation :

- Votre Compte AWS carte d'identité. Si vous Compte AWS faites partie d'une AWS organisation, vous avez également besoin de l'ID du compte de gestion.
- L'ID réseau Ariba (ANID) de votre système SAP Ariba.

> **Note**
>
> Pour plus d'informations sur les ANID dans Ariba et pour obtenir des réponses à d'autres questions concernant Ariba, consultez la page Ariba Network for Suppliers : Frequently Asked Questions sur le site Web de SAP Ariba.

Pour configurer en vue AWS Marketplace de l'intégration à Ariba

1. Dans AWS MarketplaceGérer les systèmes d'approvisionnement, sous Systèmes d'approvisionnement, choisissez Configurer l'intégration Ariba.
2. Sur la page Gérer l'intégration SAP Ariba, sous Informations sur le compte, entrez le nom et la description de votre intégration, ainsi que l'identifiant réseau SAP Ariba (ANID) de votre système Ariba.

   > **Note**
   >
   > Vous souhaiterez peut-être que vos factures dans la AWS Billing console fassent référence au bon de commande cXML utilisé pour vous abonner à votre produit contractuel SaaS. Si tel est le cas, vous pouvez activer l'intégration de facturation à l'aide d'un rôle lié à un service dans les AWS Marketplace paramètres.

3. Assurez-vous que le mode Test est activé, puis sélectionnez Enregistrer pour enregistrer vos paramètres AWS Marketplace d'intégration.
4. Contactez-nous pour démarrer le processus de création de votre intégration SAP Ariba. Incluez les informations ci-dessus. AWS Marketplacevous envoie des instructions pour configurer et tester votre intégration Ariba.

> **Note**
>
> Vous devez disposer d'un accès administrateur à votre système SAP Ariba pour créer la relation fournisseur avecAWS Marketplace.

En suivant les instructions et les paramètres de configuration de l'AWS Marketplaceéquipe, vous créez l'intégration dans votre environnement de test SAP Ariba, en l'AWS Marketplaceexécutant en mode test. Dans l'environnement de test, les demandes d'abonnement sont envoyées au backend Ariba afin que vous puissiez voir le flux complet, y compris les approbations, sans créer d'abonnementAWS Marketplace, et aucune facture n'est générée. Cette approche permet de tester la configuration avant d'activer le poinçonnage en production. Une fois vos tests terminés et que vous êtes prêt à passer à la production, contactez-nous pour configurer le compte dans l'environnement de production.

> **Note**
>
> N'oubliez pas de passer à la production lorsque vous aurez terminé de tester votre intégration. Dans le cas contraire, les utilisateurs de votre système penseront qu'ils sont en train de créer des demandes, mais aucun logiciel ne sera acheté.

Lorsque vos tests sont terminés et que vous avez travaillé avec l'AWS Marketplaceéquipe pour désactiver le mode test, votre intégration est terminée.

Pour plus d'informations sur la configuration de SAP Ariba, consultez les rubriques suivantes de SAP Ariba :

- SAP Ariba PunchOut sur le site Web de SAP Ariba
- Présentation de SAP Ariba PunchOut sur le site Web de la communauté SAP

> **Note**
>
> Pour plus d'informations sur les codes UNSPSC utilisés parAWS Marketplace, reportez-vous à la section. Codes UNSPSC utilisés par AWS Marketplace

Codes UNSPSC utilisés par AWS Marketplace

AWS Marketplaceutilise le code UNSPSC (Produits et services normalisés des Nations Unies) suivant pour les listes de logiciels renvoyées au panier d'achat : 43232701

Désactivation de l'intégration du système d'approvisionnement

Pour désactiver l'intégration avec Coupa ou SAP Ariba, vous devez supprimer l'intégration Punchout du système d'approvisionnement. Pour ce faire, désactivez la fonctionnalité de redirection automatique AWS Marketplace depuis Coupa ou Ariba. Cela désactive l'intégration, mais conserve les paramètres et permet de la réactiver facilement.

Si vous devez supprimer complètement la configuration d'intégration située sur le AWS Marketplace côté, vous devez nous contacter.

Essais gratuits

Certains produits énumérés sur la liste AWS Marketplace offrent des essais gratuits. L'essai gratuit vous permet d'essayer le logiciel avant de l'acheter. Les essais gratuits sont limités à un certain nombre d'utilisations gratuites ou pour une durée spécifique. Vous ne pouvez pas suspendre une période d'essai gratuite une fois qu'elle a commencé.

Tarification des logiciels et de l'infrastructure

Les essais gratuits proposés par les vendeurs ne s'appliquent qu'au prix du logiciel de leur produit répertorié surAWS Marketplace. Les acheteurs sont responsables de tous les coûts d'infrastructure liés à l'utilisation du produit du vendeur,AWS Marketplace que le prix du logiciel inclue ou non un essai gratuit. Ces coûts d'infrastructure sont définis parAWS et sont disponibles sur leurs pages de tarification respectives. Par exemple, si vous vous abonnez à un produit Amazon Machine Image (AMI) bénéficiant d'un essai gratuit, l'utilisation de l'AMI ne vous sera pas facturée pendant l'essai gratuit. Toutefois, vous pouvez être facturée pour l'instance Amazon Elastic Compute Cloud (Amazon EC2) sur laquelle vous exécutez le produit AMI.

> **Note**
>
> Certains produits peuvent nécessiter uneAWS infrastructure supplémentaire pour fonctionner. Par exemple, les vendeurs peuvent fournir des instructions de déploiement ou des modèles permettant de déployer des équilibreurs de charge, du stockage, des bases de données ou autresServices AWS dans votreCompte AWS. Pour comprendre ce queServices AWS le vendeur a exigé pour son produit, consultez les pages détaillées des produits répertoriés surAWS Marketplace. Ensuite, consultez les pages de tarification de ceux-ciServices AWS.

Essais gratuits pour les produits basés sur l'AMI

Certains produits AMI proposés à l'heure ou à l'heure avec une tarification annuelleAWS Marketplace proposent des essais gratuits. Lorsque vous vous abonnez à un essai gratuit, vous pouvez exécuter une instance Amazon EC2 du produit AMI pendant une durée définie par le vendeur sans avoir à payer de frais logiciels horaires. Vous êtes responsable des frais d'infrastructure. Le lancement d'instances Amazon EC2 supplémentaires entraînera des frais logiciels horaires par instance. Les essais gratuits sont automatiquement convertis en un abonnement payant à l'expiration.

Si vous ne résiliez pas l'instance Amazon EC2 avant la fin de l'essai gratuit, vous devrez payer des frais logiciels horaires à la fin de l'essai gratuit. La désinscription à l'essai gratuit ne met pas automatiquement fin à vos instances Amazon EC2 et vous devrez payer des frais logiciels pour toute utilisation continue. Pour plus d'informations sur les frais d'infrastructure, consultez Tarification Amazon EC2.

Essais gratuits pour les produits en contenants

Certains produits en conteneur proposés à l'heure ou à l'heure avec une tarification à long termeAWS Marketplace font l'objet d'essais gratuits. Lorsque vous vous abonnez à un essai gratuit, vous pouvez exécuter plusieurs tâches Amazon Elastic Container Service (Amazon ECS) ou des modules Amazon Elastic Kubernetes Service (Amazon EKS) pendant une durée sans avoir à payer de frais logiciels horaires. Le nombre de tâches ou de modules inclus et la durée de l'essai gratuit sont définis par le vendeur. Vous êtes responsable des frais d'infrastructure. Le lancement de tâches ou de modules supplémentaires au-delà du nombre inclus dans l'essai gratuit entraînera des frais logiciels horaires par tâche ou module. Les essais gratuits sont automatiquement convertis en un abonnement payant à l'expiration.

Si vous ne mettez pas fin à la tâche ou au module avant la fin de l'essai gratuit, vous devrez payer des frais logiciels horaires à la fin de l'essai gratuit. La désinscription à l'essai gratuit ne met pas automatiquement fin à vos tâches ou à vos modules, et vous devrez payer des frais logiciels pour toute utilisation continue. Pour plus d'informations sur les frais d'infrastructure, consultez les tarifs Amazon ECS et Amazon EKS.

Essais gratuits pour les produits de Machine Learning

Certains produits d'apprentissage automatique proposés à l'heureAWS Marketplace proposent des essais gratuits. Lorsque vous vous abonnez à un essai gratuit, vous pouvez gérer des SageMaker terminaux Amazon, des tâches de transformation par lots ou des tâches de formation pour une durée définie par le vendeur sans avoir à payer de frais logiciels horaires. Vous êtes responsable des frais d'infrastructure. Les essais gratuits sont automatiquement convertis en un abonnement payant à l'expiration.

Si vous ne résiliez aucun terminal Amazon SageMaker , aucun poste de transformation par lots ou aucun poste de formation avant la fin de l'essai gratuit, vous devrez payer des frais logiciels horaires à la fin de l'essai gratuit. La désinscription à l'essai gratuit ne met pas automatiquement fin à vos SageMaker terminaux Amazon, à vos tâches de transformation par lots ou à vos tâches de formation,

et vous devrez payer des frais logiciels pour toute utilisation continue. Pour plus d'informations sur les frais d'infrastructure, consultez les SageMaker tarifs d'Amazon.

Essais gratuits pour les produits SaaS

Les produits SaaS (Software as a Service) proposentAWS Marketplace des essais gratuits. Les essais gratuits du SaaS ne se transforment pas automatiquement en contrats payants. Si vous n'avez plus besoin de la version d'essai gratuite, vous pouvez la laisser expirer. Pour plus d'informations, consultez Essais gratuits de SaaS.

Utilisation du niveau gratuit d'AWS avec AWS Marketplace.

Pour aider les nouveaux Amazon Web Services (AWS) démarrer dans le cloud, AWS à instauré un niveau d'offre gratuite. L'offre gratuite d'AWS peut être utilisée pour n'importe quelle action à exécuter dans le cloud : lancer de nouvelles applications, tester des applications existantes dans le cloud ou, plus simplement, vous familiariser avec AWS. À l'expiration de l'offre d'utilisation gratuite (ou si votre utilisation de l'application dépasse les limites du niveau d'offre gratuite), vous devrez simplement vous acquitter des frais standard applicables, pay-as-you-go les frais de service. Pour de plus amples informations, veuillez consulter Offre gratuite d'AWS.

Les clients du niveau gratuit d'AWS peuvent bénéficier d'une utilisation gratuite des logiciels d'AWS Marketplace, dans la limite de 750 heures d'Amazon Elastic Compute Cloud (Amazon EC2) chaque mois pendant un an. Consultez AWS Marketplace pour démarrer.

Ajout d'abonnements AWS Marketplace à AWS Service Catalog

permet aux organisations de créer et gérer des catalogues des Service Catalog informatiques dont l'utilisation est approuvée sur Amazon Web Services () et gérer des catalogues des services informatiques dont l'utilisation est approuvée sur Amazon Web Services (AWS). Ces services informatiques peuvent comprendre toutes les solutions depuis les images de machine virtuelle, les serveurs, les logiciels et les bases de données, jusqu'aux architectures d'application à plusieurs niveaux complètes. Le Service Catalog vous permet de gérer de manière centralisée les services informatiques couramment déployés. Service Catalog vous aide à assurer une gouvernance cohérente et à répondre à vos exigences de conformité, tout en permettant aux utilisateurs de déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin.

Pour plus d'informations, consultez la section AjouterAWS Marketplace des produits à votre portefeuille dans le Guide de l'administrateur du Service Catalog.

Commentaires sur les produits

AWS Marketplace souhaite que les acheteurs aient accès aux informations dont ils ont besoin pour faire des choix d'achat intelligents. En tant que client AWS, vous pouvez soumettre des avis écrits pour les articles répertoriés dansAWS Marketplace. Nous vous encourageons à partager votre avis, favorable ou défavorable.

> **Note**
>
> Les produits de données ne prennent pas en charge les révisions de produits.

Consignes

Toute personne possédant unAWS Marketplacel'abonnement à un produit peut créer un avis pour celui-ci. Utilisez les instructions suivantes pour rédiger des avis sur les produits :

- Inclure les raisons— Les meilleures critiques indiquent non seulement si vous avez aimé ou non un produit, mais aussi pourquoi. Vous pouvez discuter des produits associés et de la façon dont cet élément peut leur être comparé.
- Soyez précis— Concentrez-vous sur les caractéristiques spécifiques du produit et sur votre expérience avec celui-ci. Pour les avis par vidéo, écrivez une brève introduction.
- Soyez concis— Les critiques écrites doivent comporter au moins 20 mots et sont limitées à 5 000 mots. La longueur idéale est de 75 à 500 mots.
- Sois sincère— Votre opinion honnête sur le produit, positive ou négative, est appréciée. Toutes les informations utiles peuvent aider les clients à prendre leurs décisions d'achat.
- Soyez transparent— Si vous avez reçu un produit gratuit en échange de votre avis, indiquez-le clairement et visiblement.

Restrictions

AWS se réserve le droit de supprimer les commentaires qui incluent l'un des contenus suivants.

- Contenu offensant, notamment :
  - Contenu obscène ou de mauvais goût

  - Remarques grossières ou malveillantes
  - Promotion de conduites illégales ou immorales
- Contenu promotionnel, notamment :
  - Publicités, supports promotionnels, commentaires récurrents qui insistent sur le même point
  - Sentiments émis par ou au nom d'une personne ou d'une entreprise ayant un intérêt financier dans le produit ou un produit directement concurrent (y compris les commentaires des auteurs, des éditeurs, des fabricants ou des marchands tiers qui vendent le produit)
  - Avis écrits pour toute forme de compensation autre qu'une copie gratuite du produit, y compris les avis qui font partie d'un package publicitaire payant
  - Les commentaires écrits par un client sans abonnement vérifiable au produit.
- Contenu inapproprié, notamment :
  - Contenu copié à partir d'autres personnes, y compris des citations excessives
  - Informations de contact ou URL externes à Amazon.com
  - Détails sur la disponibilité ou autre commande/expédition
  - Vidéos avec filigranes
  - Remarques sur d'autres commentaires visibles sur la page, la visibilité sur la page étant susceptible de changer sans préavis
  - Contenu en langue étrangère, sauf s'il y a un lien évident avec le produit
  - Texte avec des problèmes de formatage
- Informations hors sujet, notamment :
  - Retours sur le vendeur ou sur votre expérience d'expédition
  - Commentaires sur des fautes de frappe ou des inexactitudes dans notre catalogue ou la description du produit (utilisez pour cela le formulaire au bas de la page du produit)

Pour toute question sur les commentaires des clients, contactez-nous.

Délais et attentes

Nous nous efforçons de traiter les évaluations des produits aussi rapidement que possible. Cependant,AWS Marketplacel'équipe doit communiquer à la fois avec l'évaluateur et le vendeur pour confirmer et vérifier la validité de l'évaluation par rapport à notrethe section called “Consignes”etthe section called “Restrictions”. Nous suivons la même voiecalendrier et attentesdes conseils décrits dans leAWS MarketplaceGuide du vendeurpour le temps nécessaire pour terminer le processus.

Obtention de support

En cas de problèmes généraux sur AWS Marketplace, contactez-nous. Pour toute question sur les logiciels que vous achetez via AWS Marketplace, contactez le vendeur.

AWS Marketplace Vendor Insights

AWS MarketplaceVendor Insights simplifie les évaluations des risques logiciels en vous aidant à vous procurer des logiciels fiables et conformes aux normes de votre secteur. Avec AWS Marketplace Vendor Insights, vous pouvez surveiller le profil de sécurité d'un produit en temps quasi réel à partir d'une interface utilisateur unique. Il réduit vos efforts d'évaluation en fournissant un tableau de bord contenant les informations de sécurité d'un produit logiciel. Vous pouvez utiliser le tableau de bord pour consulter et évaluer des informations, telles que la confidentialité des données, la sécurité des applications et le contrôle d'accès.

AWS MarketplaceVendor Insights collecte des données de sécurité auprès des vendeurs et aide les acheteurs en leur fournissant des logiciels fiables qui répondent en permanence aux normes du secteur. En s'intégrant àAWS Audit Manager, AWS Marketplace Vendor Insights peut automatiquement extraire les informations de up-to-date sécurité de vos produits SaaS (Software as a Service)AWS Marketplace. AWS Marketplace Vendor Insights s'intègre à AWS Artifact des rapports tiers afin que vous puissiez accéder aux rapports de conformité à la demande pour les logiciels de votre fournisseur, ainsi qu'aux rapports pourServices AWS.

AWS MarketplaceVendor Insights fournit des informations fondées sur des preuves issues de 10 catégories de contrôle et de plusieurs contrôles. Il rassemble les informations fondées sur des preuves provenant de trois sources :

- Comptes de production du fournisseur — Parmi les multiples contrôles, 25 contrôles permettent de recueillir des preuves en temps réel à partir des comptes de production d'un fournisseur. Les preuves réelles de chaque contrôle sont générées par une ou plusieurs AWS Config règles qui évaluent les paramètres de configuration des AWS ressources d'un vendeur. Les preuves réelles sont la méthode qui permet de mettre régulièrement à jour les données provenant de sources multiples afin de présenter les informations les plus récentes. AWS Audit Managercapture les preuves et les transmet au tableau de bord AWS Marketplace Vendor Insights.
- Rapports ISO 27001 et SOC 2 de type II du fournisseur — Les catégories de contrôle sont mappées aux contrôles des rapports de l'Organisation internationale de normalisation (ISO) et du contrôle de l'organisation des services (SOC) 2. Lorsque les vendeurs partagent ces rapports avec AWS Marketplace Vendor Insights, le service extrait les données pertinentes et les présente dans le tableau de bord.
- Auto-évaluation des fournisseurs : les vendeurs effectuent une auto-évaluation. Ils peuvent également créer et télécharger d'autres types d'auto-évaluation, notamment l'auto-évaluation de la

sécurité de AWS Marketplace Vendor Insights et le questionnaire Consensus Assessment Initiative (CAIQ).

La vidéo suivante montre comment simplifier l'évaluation des risques liés au SaaS et utiliser AWS Marketplace Vendor Insights.

Commencer à utiliser AWS Marketplace Vendor Insights en tant qu'acheteur

AWS MarketplaceVendor Insights présente des informations de sécurité pour les produits logiciels disponibles dansAWS Marketplace. Vous pouvez utiliser AWS Marketplace Vendor Insights pour consulter les profils de sécurité des produits dansAWS Marketplace.

Le tableau de bord AWS Marketplace Vendor Insights présente les artefacts de conformité et les informations de contrôle de sécurité d'un produit logiciel à l'aide de AWS Marketplace Vendor Insights pour évaluer le produit. AWS Marketplace Vendor Insights rassemble les informations fondées sur des preuves pour les multiples contrôles de sécurité présentés sur le tableau de bord.

L'utilisation de AWS Marketplace Vendor Insights pour accéder aux informations de sécurité et de conformité des produits est gratuite.

Trouvez des produits grâce à AWS Marketplace Vendor Insights

Vous pouvez consulter le profil et le résumé d'un produit sur le tableau de bord AWS Marketplace Vendor Insights ou sélectionner les contrôles de catégorie pour en savoir plus sur les données collectées sur le produit. Pour rechercher des produits dans AWS Marketplace AWS Marketplace Vendor Insights, suivez la procédure suivante.

Pour trouver des produits avec AWS Marketplace Vendor Insights

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Choisissez Afficher tous les produits.
3. Afficher les produits dotés de la balise Vendor Insights.
4. Sous Affiner les résultats pour Vendor Insights, sélectionnez Profils de sécurité.
5. Sur la page détaillée du produit, sous Aperçu du produit, choisissez la section Vendor Insights.
6. Choisissez Afficher tous les profils pour ce produit.

7. Vous pouvez consulter les détails du produit dans l'aperçu ainsi que la liste des certificats de sécurité reçus.
8. Choisissez Demander l'accès.
9. Sur la page Demander l'accès aux données Vendor Insight, fournissez vos informations, puis choisissez Demander un accès.

   Un message de confirmation apparaît, indiquant que vous avez correctement demandé l'accès aux données AWS Marketplace Vendor Insights pour ce produit.

Demandez l'accès aux données d'évaluation en vous abonnant

Avec AWS Marketplace Vendor Insights, vous pouvez surveiller en permanence le profil de sécurité des logiciels des fournisseurs. Tout d'abord, abonnez-vous ou demandez l'accès aux données d'évaluation des fournisseurs pour le produit que vous souhaitez surveiller. Si vous ne souhaitez plus contrôler les données d'évaluation d'un produit, vous pouvez vous désabonner de ses données d'évaluation. L'utilisation de AWS Marketplace Vendor Insights pour accéder aux informations de sécurité et de conformité des produits est gratuite. Pour plus d'informations sur la tarification, consultez la section Tarification de AWS Marketplace Vendor Insights.

Pour avoir accès à toutes les données d'évaluation d'un produit d'un fournisseur spécifique, vous devez vous abonner aux données d'évaluation du produit.

Pour s'abonner aux données d'évaluation de AWS Marketplace Vendor Insights pour un produit

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Choisissez Vendor Insights.
3. Dans Vendor Insights, choisissez un produit.
4. Choisissez l'onglet Overview (Présentation).
5. Choisissez Demander l'accès.
6. Entrez vos informations dans les champs prévus à cet effet.
7. Lorsque vous avez terminé, choisissez Demander l'accès.

   Un message de confirmation apparaît indiquant que vous avez demandé l'accès à toutes les données d'évaluation des fournisseurs pour ce produit.

Se désabonner des données d'évaluation

Si vous ne souhaitez plus accéder aux données d'évaluation d'un produit d'un fournisseur, vous pouvez vous désabonner des données d'évaluation du produit.

Pour vous désabonner des données d'évaluation de AWS Marketplace Vendor Insights pour un produit

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Choisissez Vendor Insights.
3. Sur la page détaillée du produit, choisissez un produit, puis cliquez sur Se désabonner.
4. Lisez les conditions associées au désabonnement aux données AWS Marketplace Vendor Insights.
5. Tapez **`Unsubscribe`** dans le champ de saisie de texte, puis choisissez Se désabonner.

   Un message de confirmation apparaît, indiquant que vous vous êtes désinscrit des données AWS Marketplace Vendor Insights et que l'accès ne vous sera plus facturé.

Consulter le profil de sécurité d'un produit avec AWS Marketplace Vendor Insights

AWS MarketplaceVendor Insights collecte des données de sécurité auprès des vendeurs. Le profil de sécurité d'un produit affiche des informations actualisées sur la sécurité, la résilience, la conformité du produit et d'autres facteurs nécessaires à votre évaluation. Ces informations aident les acheteurs comme vous en vous aidant à vous procurer des logiciels fiables qui répondent en permanence aux normes du secteur. Pour chaque produit SaaS qu'il évalue, AWS Marketplace Vendor Insights recueille des informations factuelles pour de multiples contrôles de sécurité.

Rubriques

- Tableau de bord dans AWS Marketplace Vendor Insights
- Afficher le profil de sécurité d'un produit SaaS
- Comprendre les catégories de contrôle

Tableau de bord dans AWS Marketplace Vendor Insights

Le tableau de bord présente les artefacts de conformité et les informations de contrôle de sécurité d'un produit logiciel collectées par AWS Marketplace Vendor Insights. Des informations fondées sur des preuves pour toutes les catégories de contrôle de sécurité sont fournies, telles qu'un changement de résidence des données ou l'expiration de la certification. Le tableau de bord consolidé fournit les modifications des informations de conformité. AWS Marketplace Vendor Insights vous évite d'avoir à créer des questionnaires supplémentaires et à utiliser un logiciel d'évaluation des risques. Grâce à un tableau de bord régulièrement mis à jour et validé, vous pouvez surveiller en permanence le contrôle de sécurité du logiciel après l'achat.

Afficher le profil de sécurité d'un produit SaaS

AWS MarketplaceVendor Insights vous aide à prendre des décisions concernant le logiciel d'un vendeur. AWS Marketplace Vendor Insights extrait des données à partir des informations factuelles d'un vendeur dans 10 catégories de contrôle et plusieurs contrôles. Vous pouvez consulter le profil et le résumé d'un produit SaaS sur le tableau de bord ou sélectionner des catégories de contrôle pour en savoir plus sur les données collectées. Vous devez être abonné au produit et avoir accès pour consulter les informations de conformité via le profil.

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. Choisissez Vendor Insights.
3. Dans Vendor Insights, choisissez un produit.
4. Sur la page de détail du profil, choisissez l'onglet Sécurité et conformité.

   > **Note**
   >
   > Un chiffre dans un cercle rouge indique le nombre de contrôles non conformes.

5. Pour les catégories de contrôle, choisissez le texte sous l'une des catégories répertoriées pour afficher plus d'informations.

   - Choisissez le premier nom de contrôle (Disposez-vous d'une politique/procédure garantissant le respect des exigences législatives, réglementaires et contractuelles applicables ?).
   - Lisez les informations présentées. Vous pouvez également consulter les rapports provenant de rapports AWS Artifact tiers ou consulter les exceptions émanant de l'auditeur.

- Sélectionnez le nom du produit dans le menu de navigation ci-dessus pour revenir à la page détaillée du produit.

Comprendre les catégories de contrôle

AWS MarketplaceVendor Insights vous fournit des informations factuelles issues de plusieurs contrôles répartis dans 10 catégories de contrôle. AWS Marketplace Vendor Insights rassemble les informations provenant de trois sources : les comptes de production des fournisseurs, l'auto-évaluation des fournisseurs et les rapports ISO 27001 et SOC 2 Type II des fournisseurs. Pour plus d'informations sur ces sources, consultezAWS Marketplace Vendor Insights.

La liste suivante fournit une description de chaque catégorie de contrôle :

Gestion de l'accès

Identifie, suit, gère et contrôle l'accès à un système ou à une application.

Sécurité des applications

Vérifie si la sécurité a été intégrée à l'application lors de sa conception, de son développement et de son test.

Politique d'audit, de conformité et de sécurité

Évalue la conformité d'une organisation aux exigences réglementaires.

Résilience et continuité de l'activité

Évalue la capacité de l'organisation à s'adapter rapidement aux perturbations tout en maintenant la continuité des activités.

Sécurité des données

Protège les données et les actifs.

Sécurité de l'appareil de l'utilisateur final

Protège les appareils portables des utilisateurs finaux et les réseaux auxquels ils sont connectés contre les menaces et les vulnérabilités.

Ressources humaines

Évalue la gestion des données sensibles par la division liée aux employés lors de processus tels que l'embauche, le paiement et le licenciement des employés.

Sécurité de l'infrastructure

Protège les actifs critiques contre les menaces et les vulnérabilités.

Gestion des risques et réponse aux incidents

Évalue le niveau de risque jugé acceptable et les mesures prises pour répondre aux risques et aux attaques.

Politique de sécurité et de configuration

Évalue les politiques de sécurité et les configurations de sécurité qui protègent les actifs d'une organisation.

Ensembles de catégories de contrôle

Les tableaux suivants fournissent des informations détaillées pour chaque catégorie ainsi que des informations sur les valeurs collectées pour chaque catégorie. La liste suivante décrit le type d'informations dans chaque colonne du tableau :

- Ensemble de contrôles : les contrôles sont affectés à un ensemble de contrôles, et chaque contrôle reflète la fonction de sécurité de sa catégorie. Chaque catégorie possède plusieurs ensembles de contrôles.
- Nom du contrôle : nom de la politique ou de la procédure. « Nécessite une attestation manuelle » signifie qu'une confirmation écrite ou une documentation de la politique ou de la procédure est requise.
- Description du contrôle — Questions, informations ou documentation nécessaires concernant cette politique ou procédure.
- Détails de l'extraction des preuves — Informations et contexte nécessaires sur le contrôle pour obtenir davantage les données nécessaires pour cette catégorie.
- Valeur d'échantillon : exemple donné à titre indicatif pour expliquer à quoi pourrait ressembler une valeur de conformité pour cette catégorie afin qu'elle soit conforme aux normes réglementaires.

Rubriques

- Contrôles de sécurité des données
- Contrôles de sécurité des appareils de l'utilisateur final
- Contrôles des ressources humaines
- Contrôles de sécurité de l'infrastructure
- Gestion des risques et contrôles de réponse aux incidents
- Contrôles des politiques de sécurité et de configuration

Contrôles de gestion des accès

Les contrôles de gestion des accès identifient, suivent, gèrent et contrôlent l'accès à un système ou à une application. Ce tableau répertorie les valeurs et les descriptions des contrôles de gestion d'accès.

Kit de commande	Titre du contrôle	Description du contrôle
Authentification sécurisée	Gestion des accès 3.1.1 - Authentif ication sécurisée - Entrée de données personnelles UserId (nécessite une attestation manuelle)	Avez-vous besoin de données pers que le nom ou l'adresse e-mail) da teur ?
	Gestion des accès 3.1.2 - Authentif ication sécurisée - L'application prend en charge l'authentification à deux facteurs (nécessite une attestation manuelle)	L'application prend-elle en charge deux facteurs ?
	Gestion des accès 3.1.3 - Authentif ication sécurisée - Verrouillage du compte (nécessite une attestation manuelle)	Le compte du client est-il verrouillé plusieurs connexions ?
Gestion des accréditations	Gestion des accès 3.2.1 - Gestion des informations d'identification - Politique de mot de passe	L'application applique-t-elle une po matière de mots de passe ?

Kit de commande	Titre du contrôle	Description du contrôle
	Gestion des accès 3.2.2 - Gestion des informations d'identification - Chiffrement des mots de passe	La politique en matière de mots de que les informations de connexion nom d'utilisateur) soient cryptées p et hachées avec du sel lors de leu
	Gestion des accès 3.2.3 - Gestion des informations d'identification - Gestion des secrets	Utilisez-vous un service de gestion
	Gestion des accès 3.2.4 - Gestion des informations d'identification - Informations d'identification dans le code (nécessite une attestation manuelle)	Les informations d'identification so dans le code ?
Accès à l'environnement de production	Gestion des accès 3.3.1 - Accès à l'environnement de production - Authentification unique (nécessite une attestation manuelle)	Le SSO est-il activé pour accéder de production ?
	Gestion des accès 3.3.2 - Accès à l'environnement de production - Authentification à deux facteurs	L'authentification à deux facteurs e pour accéder à l'environnement de hébergé ?
	Gestion des accès 3.3.3 - Accès à l'environnement de production - Utilisateur root (nécessite une attestation manuelle)	L'utilisateur root est-il utilisé unique exception pour accéder à l'environ production ?

Kit de commande	Titre du contrôle	Description du contrôle
	Gestion des accès 3.3.4 - Accès à l'environnement de production - MFA pour utilisateur root	L'utilisateur root a-t-il besoin d'une multifactorielle (MFA) ?
	Gestion des accès 3.3.5 - Accès à l'environnement de production - Accès à distance	L'accès à distance à l'environneme est-il sécurisé à l'aide de mécanisn canaux cryptés ou une authentifica
Politique de contrôle d'accès	Gestion des accès 3.4.1 - Politique de contrôle d'accès - Accès avec le moindre privilège	Respectez-vous la politique du mo que les utilisateurs accèdent à l'en production ?
	Gestion des accès 3.4.2 - Politique de contrôle d'accès - Révision de la politique d'accès	Toutes les politiques d'accès de l'e production sont-elles régulièremen
	Gestion des accès 3.4.3 - Politique de contrôle d'accès - Configuration des utilisateurs et de la politique de sécurité (nécessite une attestation manuelle)	L'application permet-elle aux client utilisateurs et leurs privilèges ?
	Gestion des accès 3.4.4 - Politique de contrôle d'accès - Segmentation logique (nécessite une attestation manuelle)	Existe-t-il une segmentation logiqu des applications ?
	Gestion des accès 3.4.5 - Politique de contrôle d'accès - Révision de l'accès en cas de résiliation	Toutes les politiques d'accès pertir mises à jour lors du licenciement o de rôle de l'employé ?

Kit de commande	Titre du contrôle	Description du contrôle
Journaux d'accès	Gestion des accès 3.5.1 - Journaux d'accès	Enregistrez-vous les activités effec utilisateurs individuels dans l'enviro production ?

Contrôles de sécurité des applications

Les contrôles de sécurité des applications vérifient si la sécurité a été intégrée à l'application lors de sa conception, de son développement et de son test. Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de sécurité des applications.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Cycle de vie de développement logiciel sécurisé	Sécurité des applications 4.1.1 - Cycle de développement logiciel sécurisé - Environnement distinct	L'environnement de développement, de test et de préparation est-il distinct de l'environnement de production ?	Spécifiez si l'environnement de développement, de test et de préparation est distinct de l'environnement de production.	Oui
	Sécurité des applications 4.1.2 - Cycle de développement logiciel sécurisé - Pratique de codage sécurisé	Les ingénieurs en sécurité travaillent-ils avec les développeurs sur les pratiques de sécurité ?	Spécifiez si les développeurs et l'ingénieur en sécurité travaillent ensemble sur des pratiques de codage sécurisées.	Oui
	Sécurité des applications	Les données clients sont-	Les données clients sont-	Non

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	4.1.3 - Cycle de vie sécurisé du développement logiciel - Utilisation des données client dans un environnement de test (nécessite une attestation manuelle)	elles déjà utilisées dans les environnements de test, de développement ou d'assurance qualité ?	elles déjà utilisées dans les environnements de test, de développement ou d'assurance qualité ? Dans l'affirmative, quelles sont les données utilisées et à quoi servent-elles ?	
	Sécurité des applications 4.1.4 - Cycle de développement logiciel sécurisé - Connexion sécurisée	Le protocole SSL/TLS est-il activé pour toutes les pages Web et communications utilisant les données des clients ?	Spécifiez si une connexion sécurisée (telle que SSL/TLS) est utilisée pour toutes les communications avec les données du client.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Application Security 4.1.5 - Cycle de développement logiciel sécurisé - Image Backup	Les instantanés des images de l'application sont-ils sauvegardés ?	Spécifiez si les instantanés d'image (tels que les systèmes supportant l'application et les systèmes hébergeant les données des clients) sont sauvegardés. Dans l'affirmative, existe-t-il un processus garantissant que les instantanés d'image contenant des données délimitées sont autorisés avant d'être pris ? Le contrôle d'accès est-il implémenté pour les instantanés d'image ?	Oui. Les images sont sauvegardées avec l'approbation du client et de la direction.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Examen de la sécurité des applications	Sécurité des applications 4.2.1 - Révision de la sécurité des applications - Révision du code sécurisé	La révision du code sécurisé est-elle effectuée avant chaque publication ?	Spécifiez si une révision du code de sécurité est effectuée avant chaque publication.	Oui
	Sécurité des applications 4.2.2 - Examen de la sécurité des applications - Test de pénétration	Des tests de pénétration sont-ils effectués ? Pouvons-nous obtenir des rapports de tests d'intrusion ?	Spécifiez si des tests de pénétration sont effectués sur l'application. Si oui, pouvez-vous partager les 3 derniers rapports sous forme de preuves manuelles ?	Oui
	Sécurité des applications 4.2.3 - Examen de la sécurité des applications - Correctifs de sécurité	Tous les correctifs de sécurité à haut risque disponibles sont-ils appliqués et vérifiés régulièrement ?	Spécifiez si des correctifs de sécurité à haut risque sont appliqués régulièrement. Dans l'affirmative, à quelle fréquence sont-ils appliqués ?	Oui. Les correctifs de sécurité sont appliqués tous les mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des applications 4.2.4 - Examen de la sécurité des applications - Analyses de vulnérabilité sur les applications	Des analyses de vulnérabilité sont-elles effectuées régulièrement sur toutes les applications connectées à Internet et après des modifications importantes ?	Spécifiez si des analyses de vulnérabilité sont effectuées sur toutes les applications connectées à Internet. Dans l'affirmative, à quelle fréquence les analyses de vulnérabilité sont-elles effectuées ? Pouvons-nous obtenir une copie du rapport ?	Oui. Des analyses de vulnérabilité sont effectuées tous les mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des applications 4.2.5 - Examen de la sécurité des applications - Gestion des menaces et des vulnérabilités	Existe-t-il des processus pour gérer les outils d'évaluation des menaces et des vulnérabilités ainsi que les données qu'ils collectent ?	Spécifiez s'il existe des processus pour gérer les outils d'évaluation des menaces et des vulnérabilités ainsi que leurs résultats . Pourriez-vous fournir plus de détails sur la façon dont les menaces et les vulnérabilités sont gérées ?	Oui. Toutes les menaces et vulnérabilités provenant de différentes sources sont regroupées sur un seul portail. Ils sont gérés en fonction de leur sévérité.
	Sécurité des applications 4.2.6 - Examen de la sécurité des applications - Analyses anti-programmes malveillants	Une analyse anti-malware est-elle régulièrement effectuée sur le réseau et les systèmes hébergeant l'application ?	Spécifiez si une analyse anti-programme malveillant est effectuée sur le réseau et les systèmes hébergeant l'application. Si oui, à quelle fréquence est-ce fait ? Pouvez-vous fournir le rapport ?	Oui. Les analyses anti-programmes malveillants sont effectuées tous les mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Journaux des applications	Sécurité des applications 4.3.1 - Journaux des applications - Journaux des applications	Les journaux de candidature sont-ils collectés et examinés ?	Spécifiez si les journaux des applications sont collectés et examinés. Dans l'affirmative, pendant combien de temps les journaux sont-ils conservés ?	Oui. Les journaux sont conservés pendant un an.
	Sécurité des applications 4.3.2 - Journaux des applications - Accès aux journaux	Les journaux du système d'exploitation et des applications sont-ils protégés contre les modifications, les suppressions et/ou les accès inappropriés ?	Spécifiez si les journaux du système d'exploitation et des applications sont protégés contre les modifications, les suppressions et/ou les accès inappropriés. En cas de violation ou d'incident, avez-vous mis en place des processus pour détecter la perte des journaux des applications ?	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des applications 4.3.3 - Journaux des applications - Données stockées dans des journaux (nécessite une attestation manuelle)	Stockez-vous les informations personnelles (PII) des clients dans des journaux ?	Spécifiez si vous stockez les informations personnelles (PII) du client dans des journaux.	Non. Aucune donnée d'identification personnelle ne sera stockée dans les journaux.
Politique de contrôle des modifications	Sécurité des applications 4.4.1 - Politique de contrôle des modifications - Tests fonctionnels et de résilience	Des tests fonctionnels et de résilience sont-ils effectués avant de publier une modification ?	Spécifiez si des tests fonctionnels et de résilience sont effectués sur l'application avant une nouvelle version.	Oui
	Sécurité des applications 4.4.2 - Politique de contrôle des modifications - Procédures de contrôle des modifications	Des procédures de contrôle des modifications sont-elles requises pour toutes les modifications apportées à l'environnement de production ?	Spécifiez si des procédures de contrôle des modifications sont en place pour toutes les modifications effectuées dans l'environnement de production.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des applications 4.4.3 - Politique de contrôle des modifications - Évitez les erreurs humaines et les risques en production	Avez-vous mis en place un processus pour vérifier que l'erreur humaine et les risques ne se répercutent pas sur la production ?	Spécifiez qu'il existe un processus permettant de vérifier que l'erreur humaine et les risques ne se répercutent pas sur la production.	Oui
	Sécurité des applications 4.4.4 - Politique de contrôle des modifications - Documenter et consigner les modifications	Documentez-vous et consignez les modifications susceptibles d'avoir un impact sur les services ?	Spécifiez si les modifications ayant un impact sur le service sont documentées et enregistrées. Dans l'affirmative, pendant combien de temps les journaux sont-ils conservés ?	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Application Security 4.4.5 - Politique de contrôle des modifications - Notification des modifications pour les acheteurs (nécessite une attestation manuelle)	Existe-t-il un processus officiel pour s'assurer que les clients sont informés avant que des modifications ne soient apportées susceptibles d'avoir une incidence sur leur service ?	Spécifiez si les clients seront avertis avant d'apporter des modifications susceptibles d'avoir un impact sur leur service. Dans l'affirmative, quel est le SLA pour informer les clients des modifications ayant un impact ?	Oui. Nous informons les clients 90 jours avant l'impact des modifications.

Contrôles d'audit et de conformité

Les contrôles d'audit et de conformité évaluent la conformité d'une organisation aux exigences réglementaires. Ce tableau répertorie les valeurs et les descriptions des contrôles d'audit et de conformité.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Certifications terminées	Audit et conformité 1.1.1 - Certifications achevées (nécessite une attestation manuelle)	Dressez la liste des certifications que vous détenez.	Spécifiez les certifications que vous détenez.	SOC2, ISO/CEI 27001

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Certification en cours	Audit et conformité 1.2.1 - Certification en cours (nécessite une attestation manuelle)	Répertoriez les certificats supplémentaires actuellement en cours d'élaboration.	Répertoriez tous les certificats supplémentaires en cours d'audit ou de révision avec une date d'achèvement estimée.	Oui. La certification PCI est en cours (ETA Q2 2022).
Procédures garantissant la conformité	Audit et conformité 1.3.1 - Procédures garantissant la conformité - Procédures garantissant la conformité	Disposez-vous d'une politique ou d'une procédure garantissant le respect des exigences législatives, réglementaires et contractuelles applicables ?	Spécifiez si vous disposez d'une politique ou d'une procédure garantissant le respect des exigences législatives, réglementaires et contractuelles applicables. Dans l'affirmative, dressez la liste des détails de la procédure et téléchargez les preuves manuelles.	Oui. Nous avons téléchargé des documents tels que SOC2, ISO/IEC 27001.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Audit et conformité 1.3.2 - Procédures garantissant la conformité - Audits pour suivre les exigences en suspens	Des audits sont-ils effectués pour suivre les exigences réglementaires et de conformité en suspens ?	Précisez si des audits sont effectués pour suivre les exigences en suspens. Dans l'affirmative, veuillez fournir des détails.	Oui, des audits sont effectués tous les mois pour suivre les exigences en suspens.
	Audit et conformité 1.3.3 - Procédures garantissant la conformité - Déviations et exceptions (nécessite une attestation manuelle)	Disposez-vous d'un processus pour gérer les écarts et les exceptions aux exigences de conformité ?	Spécifiez s'il existe un processus pour gérer les exceptions ou les écarts par rapport aux exigences de conformité. Dans l'affirmative, veuillez fournir des détails.	Oui. Nous disposons d'un journal des écarts et d'outils de signalement. Nous étudions chaque exception ou écart afin d'éviter qu'il ne se reproduise à l'avenir.

Contrôles de résilience de l'entreprise

Les contrôles de résilience de l'entreprise évaluent la capacité de l'organisation à s'adapter rapidement aux perturbations tout en maintenant la continuité des activités. Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de résilience de l'entreprise.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Résilience des entreprises	Résilience et continuité des	Les tests de basculement	Spécifiez si des tests de	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	activités 6.1.1 - Résilience des activités - Tests de basculement (nécessite une attestation manuelle)	du site sont-ils effectués au moins une fois par an ?	basculement sont effectués chaque année. Dans la négative, à quelle fréquence sont-ils effectués ?	
	Résilience et continuité des activités 6.1.2 - Résilience des activités - Analyse de l'impact sur les activités (nécessite une attestation manuelle)	Une analyse de l'impact commercial a-t-elle été réalisée ?	Spécifiez si une analyse d'impact commercial a été réalisée. Dans l'affirmative, quand a-t-il été terminé pour la dernière fois ? Fournissez des détails sur l'analyse réalisée.	Oui. Une analyse de l'impact commercial a été réalisée il y a 6 mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Résilience et continuité des activités 6.1.3 - Résilience des activités - Dépendances à l'égard de fournisseurs tiers (nécessite une attestation manuelle)	Existe-t-il des dépendances vis-à-vis de fournisseurs de services tiers essentiels (en plus d'un fournisseur de services cloud) ?	Spécifiez s'il existe une dépendance vis-à-vis de fournisseurs tiers (en plus d'un fournisseur de services cloud). Dans l'affirmative, pouvez-vous fournir des informations sur les fournisseurs ?	Non
	Résilience et continuité des activités 6.1.4 - Résilience des activités - Tests de continuité et de reprise réalisés par des tiers (nécessite une attestation manuelle)	Exigez-vous que les fournisseurs tiers disposent de leurs propres processus et exercices de reprise après sinistre ?	Spécifiez si les fournisseurs tiers doivent disposer de leurs propres processus et exercices de reprise après sinistre.	Non applicable dans cet exemple.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Résilience et continuité des activités 6.1.5 - Résilience des activités - Violation de contrat par des fournisseurs tiers (nécessite une attestation manuelle)	Les contrats avec les fournisseurs de services essentiels incluent-ils une clause de pénalité ou de correction en cas de violation de la disponibilité et de la continuité des produits vendus et expédiés par Amazon (SSA) ?	Les clauses de pénalité ou de correction en cas de violation de la disponibilité et de la continuité sont-elles incluses dans les contrats avec des fournisseurs tiers ?	Non applicable dans cet exemple.
	Résilience et continuité des activités 6.1.6 - Résilience des activités - Health du système	Disposez-vous de moniteurs ou d'alertes pour évaluer l'état du système ?	Spécifiez si des moniteurs ou des alertes sont en place pour comprendre l'état du système.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Continuité des activités	Résilience et continuité des activités 6.2.1 - Continuité des activités - Politiques/ procédures de continuité des activités	Des procédures formelles de continuité des activités sont-elles élaborées et documentées ?	Précisez si des procédures formelles sont élaborées et maintenues pour assurer la continuité des activités. Dans l'affirmative, veuillez fournir plus de détails sur les procédures.	Oui
	Résilience et continuité des activités 6.2.2 - Continuité des activités - Stratégies de réponse et de reprise	Des stratégies d'intervention et de rétablissement spécifiques sont-elles définies pour les activités prioritaires ?	Spécifiez si des stratégies de reprise et de réponse sont élaborées pour les activités et les services des clients.	Oui
	Résilience et continuité des activités 6.2.3 - Continuité des activités - Tests de continuité des activités	Réalisez-vous des tests de restauration pour garantir la continuité des activités ?	Spécifiez si vous effectuez des tests de restauration pour garantir la continuité des activités en cas de panne.	Oui. En cas de panne, les systèmes de continuité des activités seront activés dans les 2 heures.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Résilience et continuité des activités 6.2.4 - Continuité des activités - Impact sur la disponibilité dans les environnements multi-locataires (nécessite une attestation manuelle)	Limitez-vous la capacité d'un acheteur à imposer une charge susceptible d'avoir un impact sur la disponibilité pour les autres utilisateurs de votre système ?	Spécifiez si le chargement d'un acheteur peut avoir un impact sur la disponibilité pour un autre acheteur. Dans l'affirmative, quel est le seuil jusqu'auquel il n'y aura aucun impact ? Dans la négative, pouvez-vous fournir plus de détails sur la manière dont vous vous assurez que les services ne sont pas affectés pendant les périodes de pointe et au-delà ?	Oui. Seuil non disponible pour cet échantillon.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Disponibilité des applications	Résilience et continuité des activités 6.3.1 - Disponibilité des applications - Registre de disponibilité (nécessite une attestation manuelle)	Y a-t-il eu des problèmes importants liés à la fiabilité ou à la disponibilité au cours de l'année écoulée ?	Précisez s'il y a eu des problèmes importants liés à la fiabilité ou à la disponibilité au cours de l'année écoulée.	Non
	Résilience et continuité des activités 6.3.2 - Disponibilité des applications - Fenêtre de maintenance planifiée (nécessite une attestation manuelle)	Des temps d'arrêt sont-ils attendus lors de la maintenance planifiée ?	Spécifiez s'il existe une fenêtre de maintenance planifiée pendant laquelle les services peuvent être indisponibles. Dans l'affirmative, quelle est la durée du temps d'arrêt ?	Non

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Résilience et continuité des activités 6.3.3 - Disponibilité des applications - Portail des incidents en ligne (nécessite une attestation manuelle)	Existe-t-il un portail en ligne sur l'état de la réponse aux incidents qui décrit les interruptions planifiées et imprévues ?	Spécifiez s'il existe un portail d'état des incidents qui décrit les interruptions planifiées et imprévues. Dans l'affirmative, veuillez fournir des informations sur la manière dont le client peut y accéder. Combien de temps après la panne le portail sera-t-il mis à jour ?	Oui. Le client peut accéder aux informations via exemple.com.
	Résilience et continuité des activités 6.3.4 - Disponibilité des applications - Objectif de temps de restauration (nécessite une attestation manuelle)	Existe-t-il un objectif de temps de restauration (RTO) spécifique ?	Spécifiez s'il existe un objectif de temps de restauration (RTO). Si oui, pouvez-vous fournir le RTO ?	Oui, un RTO de 2 heures.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Résilience et continuité des activités 6.3.5 - Disponibilité des applications - Objectif du point de reprise (nécessite une attestation manuelle)	Existe-t-il un objectif de point de reprise (RPO) spécifique ?	Spécifiez s'il existe un objectif de point de récupération (RPO). Si oui, pouvez-vous fournir le RPO ?	Oui, un RPO d'une semaine.

Contrôles de sécurité des données

Les contrôles de sécurité des données protègent les données et les actifs. Ce tableau répertorie les valeurs et les descriptions des contrôles de sécurité des données.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Données clients ingérées	Sécurité des données 2.1.1 - Données clients ingérées (nécessite une attestation manuelle)	Créez une liste des données dont les clients ont besoin pour le fonctionnement du produit.	Décrivez toutes les données consommées par les clients. Spécifiez si des données sensibles ou confidentielles sont consommées.	Aucune donnée sensible et confidentielle n'est consommée. Ce produit ne consomme que des informations non sensibles telles que les journaux des applications, de l'infrastructure etServices AWS.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
				(AWS CloudTrail AWS Config, journaux de flux VPC)
Emplacement de stockage des données	Sécurité des données 2.2.1 - Emplacement de stockage des données (nécessite une attestation manuelle)	Où sont stockées les données des clients ? Répertoriez les pays et les régions dans lesquels les données sont stockées.	Spécifiez la liste des pays et régions dans lesquels les données sont stockées.	Ohio (États-Unis), Oregon (États-Unis), Irlande (UE)
Contrôle d'accès	Sécurité des données 2.3.1 - Contrôle d'accès - Accès des employés (nécessite une attestation manuelle)	Les employés ont-ils accès aux données clients non cryptées ?	Spécifiez si les employés ont accès aux données clients non cryptées. Dans l'affirmative, expliquez brièvement pourquoi ils ont besoin d'un accès. Si ce n'est pas le cas, expliquez brièvement comment vous contrôlez l'accès.	Non, toutes les données sont cryptées lorsqu'elles sont stockées. Les employés n'auront pas accès aux données des clients, mais uniquement aux données relatives à leur utilisation.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.3.2 - Contrôle d'accès - Application mobile (nécessite une attestation manuelle)	Les clients peuvent-ils accéder à leurs données via une application mobile ?	Spécifiez si les clients peuvent accéder à leurs données via une application mobile. Dans l'affirmative, veuillez fournir plus de détails. Comment les clients se connectent-ils ? Les informations d'identification sont-elles mises en cache par l'application ? À quelle fréquence les jetons sont-ils actualisés ?	Non, le service n'est pas accessible via une application mobile.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.3.3 - Contrôle d'accès - Pays vers lesquels les données sont transmises (nécessite une attestation manuelle)	Les données des clients sont-elles transmises à des pays autres que le pays d'origine ?	Les données des clients sont-elles transmises à des pays autres que le pays d'origine ? Dans l'affirmative, spécifiez la liste des pays dans lesquels les données clients sont transmises ou reçues.	Non
	Sécurité des données 2.3.4 - Contrôle d'accès - Les données sont-elles partagées avec des fournisseurs tiers (nécessite une attestation manuelle)	Les données clients sont-elles partagées avec des fournisseurs tiers (autres que les fournisseurs de services cloud) ?	Les données clients sont-elles partagées avec des fournisseurs tiers ? Dans l'affirmative, spécifiez la liste des fournisseurs tiers et leurs pays ou régions dans lesquels vous fournissez des données clients.	Non

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.3.5 - Contrôle d'accès - Politique de sécurité relative aux fournisseurs tiers	Avez-vous mis en place des politiques ou des procédures pour garantir que les fournisseurs tiers préservent la confidentialité, la disponibilité et l'intégrité des données clients ?	Spécifiez si vous avez mis en place des politiques ou des procédures garantissant que les fournisseurs tiers préservent la confidentialité, la disponibilité et l'intégrité des données clients. Dans l'affirmative, téléchargez un manuel ou un document décrivant les politiques ou les procédures.	Non applicable dans cet exemple.
Chiffrement des données	Sécurité des données 2.4.1 - Chiffrement des données - Chiffrement des données au repos	Toutes les données sont-elles cryptées au repos ?	Spécifiez si toutes les données sont cryptées au repos.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.4.2 - Chiffrement des données - Chiffrement des données en transit	Toutes les données sont-elles cryptées en transit ?	Spécifiez si toutes les données sont cryptées en transit.	Oui
	Sécurité des données 2.4.3 - Chiffrement des données - Algorithmes puissants (nécessite une attestation manuelle)	Utilisez-vous des algorithmes de chiffrement puissants ?	Utilisez-vous des algorithmes de chiffrement puissants ? Dans l'affirmative, spécifiez quels algorithmes de chiffrement (tels que RSA, AES 256) sont utilisés.	Oui. L'AES 256 est utilisé pour chiffrer les données.
	Sécurité des données 2.4.4 - Chiffrement des données - Clé de chiffrement unique (nécessite une attestation manuelle)	Les clients ont-ils la possibilité de générer une clé de chiffrement unique ?	Les clients peuvent-ils fournir ou générer leurs propres clés de chiffrement uniques ? Dans l'affirmative, veuillez fournir plus de détails et télécharger des preuves.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.4.5 - Chiffrement des données - Accès aux clés de chiffrement (nécessite une attestation manuelle)	Les employés sont-ils empêchés d'accéder aux clés de chiffrement d'un client ?	Spécifiez si vos employés ne peuvent pas accéder aux clés de chiffrement d'un client. Si ce n'est pas le cas, expliquez pourquoi ils ont accès aux clés des clients. Dans l'affirmative, expliquez comment l'accès est contrôlé.	Oui. Les clés cryptographiques sont stockées de manière sécurisée et font l'objet d'une rotation périodique. Les employés n'ont pas accès à ces clés.
Stockage et classification des données	Sécurité des données 2.5.1 - Stockage et classification des données - Sauvegarde des données	Sauvegardez-vous les données des clients ?	Spécifiez si vous sauvegardez les données du client. Dans l'affirmative, décrivez votre politique de sauvegarde (y compris des informations sur la fréquence des sauvegardes, l'endroit où elles sont stockées, le chiffrement des sauvegardes et la redondance).	Oui, la sauvegarde est effectuée tous les trois mois. Backup est crypté et stocké dans la même région que les données du client. L'ingénieur de support du client a accès à la restauration de la sauvegarde, mais pas aux données qu'elle contient.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.5.2 - Stockage et classification des données - Politique de contrôle d'accès aux données	Mettez-vous en œuvre des contrôles d'accès appropriés pour les données clients stockées ? Indiquez vos politiques de contrôle d'accès.	Spécifiez si des contrôles d'accès appropriés (tels que le RBAC) sont mis en œuvre pour les données clients stockées. Fournissez plus de détails et des preuves manuelles sur la manière dont vous contrôlez l'accès aux données.	Oui. Les contrôles d'accès avec le moindre privilège sont mis en œuvre pour restreindre l'accès aux données des clients.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.5.3 - Stockage et classification des données - Données de transaction (nécessite une attestation manuelle)	Les détails des transactions du client (tels que les informations de carte de paiement et les informations sur les groupes effectuant des transactions) sont-ils stockés dans une zone périmétrique ?	Spécifiez si les détails des transactions du client (tels que les informations de carte de paiement et les informations sur les groupes effectuant des transactions) seront stockés dans une zone périmétrique. Dans l'affirmative, expliquez pourquoi il doit être stocké dans la zone périmétrique.	Non

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des données 2.5.4 - Stockage et classification des données - Classification des informations	Les données clients sont-elles classées en fonction des exigences légales ou réglementaires, de la valeur commerciale et de la sensibilité aux divulgations ou modifications non autorisées ?	Spécifiez si les données client sont classées par niveau de sensibilité. Dans l'affirmative, téléchargez les preuves manuelles de cette classification.	Oui
	Sécurité des données 2.5.5 - Stockage et classification des données - Segmentation des données (nécessite une attestation manuelle)	Des fonctionnalités de segmentation et de séparation des données entre les clients sont-elles fournies ?	Spécifiez si les données des différents clients sont segmentées. Dans la négative, expliquez les mécanismes dont vous disposez pour protéger les données contre la contamination croisée.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Conservation des données	Sécurité des données 2.6.1 - Conservation des données (nécessite une attestation manuelle)	Combien de temps conservez-vous les données ?	Spécifiez la durée de conservation des données. Si la période de conservation varie en fonction de la classification et de la sensibilité des données, pouvez-vous fournir des détails sur chaque période de conservation ?	6 mois
Conservation des données après le désabonnement des acheteurs	Sécurité des données 2.6.2 - Conservation des données après le désabonnement du client (nécessite une attestation manuelle)	Combien de temps conservez-vous les données après la désinscription des acheteurs ?	Spécifiez la durée de conservation des données après la désinscription des clients.	3 mois

Contrôles de sécurité des appareils de l'utilisateur final

Les contrôles de sécurité des appareils des utilisateurs finaux protègent les appareils portables des utilisateurs finaux et les réseaux auxquels ils sont connectés contre les menaces et les vulnérabilités.

Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de sécurité des appareils des utilisateurs finaux.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Inventaire des actifs/logiciels	Sécurité des appareils de l'utilisateur final 7.1.1 - Inventaire des actifs/logiciels - Inventaire des actifs	La liste d'inventaire des actifs est-elle mise à jour régulièrement ?	Spécifiez si un inventaire des actifs est tenu à jour. Dans l'affirmative, à quelle fréquence est-il mis à jour ?	Oui. L'inventaire est mis à jour chaque semaine.
	Sécurité des appareils de l'utilisateur final 7.1.2 - Inventaire des actifs/logiciels - Inventaire des logiciels et des applications	Toutes les plateformes logicielles et applications installées sur les systèmes concernés sont-elles inventoriées ?	Spécifiez si l'inventaire de tous les logiciels et applications installés est maintenu. Dans l'affirmative, à quelle fréquence est-il mis à jour ?	Oui. L'inventaire est mis à jour chaque semaine.
Sécurité des actifs	Sécurité des appareils de l'utilisateur final 7.2.1 - Sécurité des actifs - Correctifs de sécurité	Tous les correctifs de sécurité à haut risque disponibles sont-ils appliqués et vérifiés au moins une fois par mois sur tous les appareils des utilisateurs finaux ?	Spécifiez si tous les correctifs de sécurité à haut risque sont appliqués au moins une fois par mois. Dans la négative, à quelle fréquence est-il appliqué ? Pouvez-vous fournir plus de détails sur	Oui. Nous avons une équipe de sécurité qui effectue ce processus toutes les deux semaines.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
			la façon dont vous gérez les correctifs ?	
	Sécurité des appareils de l'utilisateur final 7.2.2 - Sécurité des actifs - Sécurité des terminaux	Disposez-vous d'une solution de sécurité des terminaux ?	Spécifiez si la sécurité des terminaux est installée sur tous les appareils. Dans l'affirmative, pouvez-vous fournir plus de détails sur l'outil et sur la façon dont il est maintenu ?	Oui. Notre équipe de sécurité gère cela toutes les deux semaines à l'aide d'outils internes.
	Sécurité des appareils de l'utilisateur final 7.2.3 - Sécurité des actifs - Maintenance et réparation des actifs (nécessite une attestation manuelle)	La maintenance et la réparation des actifs organisationnels sont-elles effectuées et enregistrées, avec des outils approuvés et contrôlés ?	Spécifiez si la maintenance et la réparation des actifs sont effectuées et enregistrées à l'aide d'outils contrôlés. Dans l'affirmative, pourriez-vous fournir plus de détails sur la façon dont il est géré ?	Oui. Toutes les opérations de maintenance des appareils sont enregistrées. Cette maintenance n'entraîne pas de temps d'arrêt.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des appareils de l'utilisateur final 7.2.4 - Sécurité des actifs - Contrôle d'accès aux appareils	Le contrôle d'accès est-il activé sur les appareils ?	Spécifiez si les contrôles d'accès (tels que RBAC) sont activés sur les appareils.	Oui. L'accès avec le moindre privilège est mis en œuvre pour tous les appareils.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Journaux de l'appareil	Sécurité des appareils de l'utilisateur final 7.3.1 - Journaux des appareils - Informations suffisantes dans les journaux (nécessite une attestation manuelle)	Les informations enregistrées dans les journaux du système d'exploitation et des appareils sont-elles suffisantes pour permettre une enquête sur les incidents ?	Spécifiez si des informations suffisantes (telles que les tentatives de connexion réussies et échouées et les modifications apportées aux paramètres de configuration et aux fichiers sensibles) sont incluses dans les journaux pour faciliter l'enquête sur les incidents. Si ce n'est pas le cas, veuillez fournir plus de détails sur la manière dont vous gérez les enquêtes sur les incidents.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des appareils de l'utilisateur final 7.3.2 - Journaux des appareils - Accès aux journaux des appareils	Les journaux des appareils sont-ils protégés contre les modifications, les suppressions et/ou les accès inappropriés ?	Spécifiez si les journaux de l'appareil sont protégés contre les modifications, les suppressions et/ou les accès inappropriés. Dans l'affirmative, pouvez-vous fournir des détails sur la manière dont vous l'appliquez ?	Oui. Les modifications apportées aux journaux sont appliquées par le contrôle d'accès. Toutes les modifications apportées aux journaux donnent lieu à une alerte.
	Sécurité des appareils de l'utilisateur final 7.3.3 - Journaux des appareils - Conservation des journaux (nécessite une attestation manuelle)	Les journaux sont-ils conservés suffisamment longtemps pour enquêter sur une attaque ?	Pendant combien de temps les journaux seront-ils conservés ?	Oui, 1 an.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Gestion des appareils mobiles	Sécurité des appareils de l'utilisateur final 7.4.1 - Gestion des appareils mobiles - Programme de gestion des appareils mobiles	Existe-t-il un programme de gestion des appareils mobiles ?	Spécifiez s'il existe un programme de gestion des appareils mobiles. Dans l'affirmative, veuillez préciser quel outil est utilisé pour la gestion des appareils mobiles.	Oui. Nous utilisons des outils internes.
	Sécurité des appareils de l'utilisateur final 7.4.2 - Gestion des appareils mobiles - Accès à l'environnement de production à partir d'appareils mobiles privés (nécessite une attestation manuelle)	Le personnel est-il empêché d'accéder à l'environnement de production en utilisant des appareils mobiles privés non gérés ?	Spécifiez si les employés ne peuvent pas accéder à l'environnement de production en utilisant des appareils mobiles privés non gérés. Dans la négative, comment appliquez-vous ce contrôle ?	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité des appareils de l'utilisateur final 7.4.3 - Gestion des appareils mobiles - Accès aux données des clients à partir d'appareils mobiles (nécessite une attestation manuelle)	Les employés sont-ils empêchés d'utiliser des appareils mobiles privés non gérés pour consulter ou traiter les données des clients ?	Spécifiez si les employés ne peuvent pas accéder aux données des clients en utilisant des appareils mobiles non gérés. Si non, quel est le cas d'utilisation pour autoriser l'accès ? Comment contrôlez-vous l'accès ?	Oui

Contrôles des ressources humaines

Les contrôles des ressources humaines évaluent la gestion des données sensibles par la division chargée des employés lors de processus tels que l'embauche, le paiement et le licenciement des employés. Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de ressources humaines.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Politique des ressources humaines	Ressources humaines 9.1.1 - Politique en matière de ressource	Une vérification des antécédents est-elle effectuée avant l'embauche ?	Précisez si une vérification des antécédents est effectuée pour tous les	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	s humaines - Vérification des antécédents des employés		employés avant leur embauche.	
	Ressources humaines 9.1.2 - Politique des ressources humaines - Entente avec les employés	Un contrat de travail est-il signé avant l'embauche ?	Précisez si un contrat de travail est signé avant l'embauche.	Oui
	Ressources humaines 9.1.3 - Politique des ressources humaines - Formation en matière de sécurité pour les employés	Est-ce que tous les employés suivent régulièrement des formations de sensibilisation à la sécurité ?	Précisez si les employés suivent régulièrement une formation en matière de sécurité. Dans l'affirmative, à quelle fréquence suivent-ils une formation en matière de sécurité ?	Oui. Ils suivent une formation en matière de sécurité chaque année.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Ressources humaines 9.1.4 - Politique en matière de ressources humaines - Procédure disciplinaire en cas de non-respect des politiques	Existe-t-il un processus disciplinaire en cas de non-conformité aux politiques en matière de ressources humaines ?	Précisez s'il existe un processus disciplinaire pour non-conformité aux politiques en matière de ressources humaines.	Oui
	Ressources humaines 9.1.5 - Politique en matière de ressources humaines - Vérification des antécédents des contractants/sous-traitants (nécessite une attestation manuelle)	Des vérifications des antécédents sont-elles effectuées pour les fournisseurs, sous-traitants et sous-traitants tiers ?	Spécifiez si des vérifications des antécédents sont effectuées pour les fournisseurs, sous-traitants et sous-traitants tiers. Si oui, la vérification des antécédents est-elle effectuée régulièrement ?	Oui. La vérification des antécédents est effectuée chaque année.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Ressources humaines 9.1.6 - Politique des ressources humaines - Restitution des actifs en cas de résiliation	Existe-t-il un processus permettant de vérifier le remboursement des actifs constitutifs en cas de résiliation ?	Précisez s'il existe un processus permettant de vérifier le retour des actifs constitutifs en cas de licenciement de l'employé.	Oui

Contrôles de sécurité de l'infrastructure

Les contrôles de sécurité de l'infrastructure protègent les actifs critiques contre les menaces et les vulnérabilités. Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de sécurité de l'infrastructure.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Sécurité physique	Sécurité de l'infrastructure 8.1.1 - Sécurité physique - Accès physique aux installations	Les personnes qui ont besoin d'accéder à des actifs en personne (tels que des bâtiments, des véhicules ou du matériel) doivent-elles fournir une pièce d'identité et les informations	Spécifiez si les personnes qui ont besoin d'accéder aux actifs en personne (tels que les bâtiments, les véhicules, le matériel) sont tenues de fournir une pièce d'identité et les informations	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
		d'identification nécessaires ?	d'identification nécessaires.	
	Sécurité de l'infrastructure 8.1.2 - Sécurité physique - Sécurité physique et contrôles environnementaux en place	La sécurité physique et les contrôles environnementaux sont-ils en place dans le centre de données et les immeubles de bureaux ?	Précisez si la sécurité physique et les contrôles environnementaux sont en place pour toutes les installations.	Oui
	Sécurité de l'infrastructure 8.1.3 - Sécurité physique - Accès des visiteurs (nécessite une attestation manuelle)	Enregistrez-vous l'accès des visiteurs ?	Si les visiteurs sont autorisés à entrer dans l'établissement, les registres d'accès des visiteurs sont-ils tenus à jour ? Dans l'affirmative, pendant combien de temps les journaux sont-ils conservés ?	Oui. Les journaux seront conservés pendant un an.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Sécurité du réseau	Sécurité de l'infrastructure 8.2.1 - Sécurité du réseau - Désactivation des ports et services inutilisés (nécessite une attestation manuelle)	Tous les ports et services inutilisés sont-ils désactivés dans l'environnement et les systèmes de production ?	Spécifiez si tous les ports et services non utilisés sont désactivés dans l'environnement et les systèmes de production.	Oui
	Sécurité de l'infrastructure 8.2.2 - Sécurité du réseau - Utilisation de pare-feux	Les pare-feux sont-ils utilisés pour isoler les systèmes critiques et sensibles dans des segments de réseau distincts des segments de réseau contenant des systèmes moins sensibles ?	Spécifiez si des pare-feux sont utilisés pour isoler les segments critiques et sensibles des segments dotés de systèmes moins sensibles.	Oui
	Sécurité de l'infrastructure 8.2.3 - Sécurité du réseau - Révision des règles de pare-feu	Toutes les règles relatives aux pare-feux sont-elles régulièrement révisées et mises à jour ?	À quelle fréquence les règles de pare-feu sont-elles révisées et mises à jour ?	Oui. Les règles du pare-feu sont mises à jour tous les 3 mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Sécurité de l'infrastructure 8.2.4 - Sécurité du réseau - Systèmes de détection/ prévention des intrusions	Les systèmes de détection et de prévention des intrusions sont-ils déployés dans toutes les zones sensibles du réseau et partout où les pare-feux sont activés ?	Spécifiez si les systèmes de détection et de prévention des intrusions sont activés dans toutes les zones sensibles du réseau.	Oui
	Sécurité de l'infrastructure 8.2.5 - Sécurité du réseau - Normes de sécurité et de renforcement	Avez-vous mis en place des normes de sécurité et de renforcement pour les appareils réseau ?	Spécifiez si vous avez mis en place des normes de sécurité et de renforcement pour les périphériques réseau. Dans l'affirmative, pouvez-vous fournir plus de détails (y compris des détails sur la fréquence à laquelle ces normes sont mises en œuvre et mises à jour) ?	Oui. Les normes de sécurité et de renforcement sont mises en œuvre sur les appareils réseau tous les mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Services dans le cloud	Sécurité de l'infrastructure 8.3.1 - Services cloud - Plateformes utilisées pour héberger l'application (nécessite une attestation manuelle)	Répertoriez les plateformes cloud que vous utilisez pour héberger votre application.	Spécifiez les plateformes cloud que vous utilisez pour héberger votre application.	AWS

Gestion des risques et contrôles de réponse aux incidents

La gestion des risques et les contrôles de réponse aux incidents évaluent le niveau de risque jugé acceptable et les mesures prises pour répondre aux risques et aux attaques. Ce tableau répertorie les valeurs et les descriptions relatives aux contrôles des politiques de gestion des risques et de réponse aux incidents.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Évaluation des risques	Gestion des risques/Réponse aux incidents 5.1.1 - Évaluation des risques - Gérer et identifier les risques	Existe-t-il un processus formel axé sur l'identification et la gestion des risques d'incidents perturbateurs pour l'organisation ?	Spécifiez s'il existe un processus permettant d'identifier et de traiter les risques à l'origine d'incidents perturbateurs pour l'organisation.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.1.2 - Évaluation des risques - Processus de gestion des risques	Existe-t-il un programme ou un processus pour gérer le traitement des risques identifiés lors des évaluations ?	Précisez s'il existe un programme ou un processus pour gérer les risques et leur atténuation. Dans l'affirmative, pouvez-vous fournir plus de détails sur le processus de gestion des risques ?	Oui. Nous examinons et corrigeons régulièrement les problèmes afin de remédier aux non-conformités. Les informations suivantes sont identifiées pour tout problème affectant notre environnement : • Détails du problème identifié • Cause première • Commandes de compensation • Gravité • Propriétaire • Prochaines perspectives à court terme • La voie à suivre à long terme

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.1.3 - Évaluation des risques - Évaluations des risques	Les évaluations des risques sont-elles effectuées fréquemment ?	Les évaluations des risques sont-elles effectuées fréquemment ? Dans l'affirmative, précisez la fréquence des évaluations des risques.	Oui. Les évaluations des risques sont effectuées tous les 6 mois.
	Gestion des risques/Réponse aux incidents 5.1.4 - Évaluation des risques - Évaluation des risques liés aux fournisseurs tiers	Des évaluations des risques sont-elles effectuées pour tous les fournisseurs tiers ?	Spécifiez si des évaluations des risques sont effectuées pour tous les fournisseurs tiers. Si oui, à quelle fréquence ?	Non applicable dans cet exemple.
	Gestion des risques/Réponse aux incidents 5.1.5 - Évaluation des risques - Réévaluation des risques en cas de modification du contrat	Des évaluations des risques sont-elles effectuées en cas de modification de la prestation de services ou des contrats ?	Précisez si des évaluations des risques seront effectuées chaque fois qu'une prestation de service ou un contrat est modifié.	Non applicable dans cet exemple.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.1.6 - Évaluation des risques - Accepter les risques (nécessite une attestation manuelle)	Existe-t-il un processus permettant à la direction d'accepter sciemment et objectivement les risques et d'approuver les plans d'action ?	Précisez s'il existe un processus permettant à la direction de comprendre et d'accepter les risques, et d'approuver les plans d'action et un calendrier pour résoudre un problème lié aux risques. Le processus inclut-il de fournir à la direction des informations détaillées sur les paramètres sous-jacents à chaque risque ?	Oui. Des détails sur la gravité du risque et les problèmes potentiels s'il n'est pas atténué sont fournis à la direction avant qu'elle n'approuve un risque.
	Gestion des risques/Réponse aux incidents 5.1.7 - Évaluation des risques - Mesures des risques (nécessite une attestation manuelle)	Avez-vous mis en place des mesures pour définir, surveiller et communiquer les indicateurs de risque ?	Spécifiez s'il existe un processus permettant de définir, de surveiller et de signaler les indicateurs de risque.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Gestion des incidents	Gestion des risques/Réponse aux incidents 5.2.1 - Gestion des incidents - Plan de réponse aux incidents	Existe-t-il un plan de réponse aux incidents officiel ?	Spécifiez s'il existe un plan de réponse aux incidents officiel.	Oui
	Gestion des risques/Réponse aux incidents 5.2.2 - Gestion des incidents - Contact pour signaler les incidents de sécurité (nécessite une attestation manuelle)	Existe-t-il un processus permettant aux clients de signaler un incident de sécurité ?	Spécifiez s'il existe un processus permettant aux clients de signaler un incident de sécurité. Dans l'affirmative, comment un client peut-il signaler un incident de sécurité ?	Oui. Les clients peuvent signaler les incidents à exemple.com.
	Gestion des risques/Réponse aux incidents 5.2.3 - Gestion des incidents - Signaler les incidents /principales activités	Décrivez-vous des activités clés ?	Décrivez-vous des activités clés ? Quel est le SLA pour signaler les activités clés ?	Oui. Toutes les activités clés seront signalées dans un délai d'une semaine.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.2.4 - Gestion des incidents - Reprise après incident	Disposez-vous de plans de reprise après sinistre ?	Spécifiez si vous avez des plans de reprise après un incident. Dans l'affirmative, pouvez-vous nous donner des détails sur les plans de redressement ?	Oui. Après un incident, le rétablissement sera effectué dans les 24 heures.
	Gestion des risques/Réponse aux incidents 5.2.5 - Gestion des incidents - Journaux mis à la disposition des acheteurs en cas d'attaque (nécessite une attestation manuelle)	En cas d'attaque, les ressources pertinentes (telles que les journaux, les rapports d'incidents ou les données) seront-elles mises à la disposition des clients ?	Les ressources pertinentes (telles que les journaux, les rapports d'incidents ou les données) liées à leur utilisation seront-elles mises à la disposition des clients en cas d'attaque ou d'incident ?	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.2.6 - Gestion des incidents - Bulletin de sécurité (Nécessite une attestation manuelle)	Disposez-vous d'un bulletin de sécurité qui décrit les dernières attaques et vulnérabilités affectant vos applications ?	Spécifiez si vous disposez d'un bulletin de sécurité décrivant les dernières attaques et vulnérabilités affectant vos applications. Dans l'affirmative, pouvez-vous fournir les détails ?	Oui. Les clients peuvent signaler les incidents à exemple.com.
Détection des incidents	Gestion des risques/Réponse aux incidents 5.3.1 - Détection des incidents - Journalisation complète	Existe-t-il une journalisation complète pour faciliter l'identification et l'atténuation des incidents ?	Spécifiez si la journalisation complète est activée. Identifiez les types d'événements que le système est capable de consigner. Combien de temps les journaux sont-ils conservés ?	Oui. Les événements suivants sont enregistrés : applications, appareils, Services AWS etc. AWS CloudTrail AWS Config, et journaux de flux VPC. Les journaux sont conservés pendant 1 an.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Gestion des risques/Réponse aux incidents 5.3.2 - Détection des incidents - Surveillance des journaux	Surveillez-vous les activités inhabituelles ou suspectes et lancez-vous des alertes à l'aide de mécanismes de détection tels que la surveillance des journaux ?	Spécifiez si une surveillance de sécurité et des alertes régulières sont effectuées. Dans l'affirmative, inclut-il la surveillance des journaux pour détecter les comportements inhabituels ou suspects ?	Oui. Tous les journaux sont surveillés pour détecter tout comportement inhabituel tel que plusieurs échecs de connexion, une connexion à partir d'une géolocalisation inhabituelle ou d'autres alertes suspectes.
	Gestion des risques/Réponse aux incidents 5.3.3 - Détection des incidents - Violation de données par un tiers	Existe-t-il un processus permettant d'identifier, de détecter et de consigner les problèmes de sécurité, de confidentialité ou de violation de données des sous-traitants ?	Spécifiez si un processus est en place pour identifier et détecter les fournisseurs ou sous-traitants tiers en cas de violation de données, de sécurité ou de confidentialité.	Oui

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
SLA pour la notification des incidents	Gestion des risques/Réponse aux incidents 5.4.1 - SLA pour la notification des incidents (nécessite une attestation manuelle)	Quel est le SLA pour l'envoi de notifications en cas d'incidents ou de violations ?	Quel est le SLA pour l'envoi de notifications en cas d'incidents ou de violations ?	7 jours

Contrôles des politiques de sécurité et de configuration

Les contrôles des politiques de sécurité et de configuration évaluent les politiques de sécurité et les configurations de sécurité qui protègent les actifs d'une organisation. Ce tableau répertorie les valeurs et les descriptions des contrôles des politiques de sécurité et de configuration.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Politiques relatives à la sécurité de l'information	Politique de sécurité et de configuration 10.1.1 - Politiques de sécurité de l'information - Politique de sécurité de l'information	Disposez-vous d'une politique de sécurité des informations détenue et gérée par une équipe de sécurité ?	Spécifiez si vous disposez d'une politique de sécurité des informations. Si oui, partagez ou téléchargez une preuve manuelle.	Oui. Nous élaborons notre politique de sécurité sur la base du framework NIST.
	Politique de sécurité et de configuration 10.1.2 - Politiques de sécurité	Toutes les politiques de sécurité sont-elles révisées chaque année ?	Spécifiez si les politiques de sécurité sont révisées chaque année. Dans	Oui. Révisé chaque année.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	de l'information - Révision des politiques		la négative, à quelle fréquence les politiques sont-elles révisées ?	
Politiques relatives aux configurations de sécurité	Politique de sécurité et de configuration 10.2.1 - Politiques relatives aux configurations de sécurité - Configurations de sécurité (nécessite une attestation manuelle)	Les normes de configuration de sécurité sont-elles maintenues et documentées ?	Spécifiez si toutes les normes de configuration de sécurité sont maintenues et documentées. Si oui, partagez ou téléchargez une preuve manuelle.	Oui
	Politique de sécurité et de configuration 10.2.2 - Politiques relatives aux configurations de sécurité - Révision des configurations de sécurité (nécessite une attestation manuelle)	Les configurations de sécurité sont-elles révisées au moins une fois par an ?	Spécifiez si les configurations de sécurité sont révisées au moins une fois par an. Dans le cas contraire, précisez la fréquence de révision.	Oui. Révisé tous les 3 mois.

Kit de commande	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	Politique de sécurité et de configuration 10.2.3 - Politiques relatives aux configurations de sécurité - Modifications apportées aux configurations	Les modifications apportées aux configurations sont-elles enregistrées ?	Spécifiez si les modifications de configuration sont enregistrées. Dans l'affirmative, pendant combien de temps les journaux sont-ils conservés ?	Oui. Toutes les modifications apportées aux configurations sont surveillées et enregistrées. Des alertes sont déclenchées lorsque les configurations sont modifiées. Les journaux sont conservés pendant 6 mois.

Exporter des instantanés en tant qu'acheteur à l'aide deAWS MarketplaceInformations sur les fournisseurs

UNinstantanéest unpoint-in-timeposture d'un profil de sécurité. L'exportation d'instantanés permet de télécharger et de consulter des données hors ligne, d'examiner des données probantes et de comparer des produits.

Exporter un instantané

Vous pouvez exporter au format JSON ou CSV. Pour exporter un instantané, procédez comme suit.

1. Connectez-vous à AWS Management Console et ouvrez la console AWS Marketplace.
2. ChoisissezInformations sur les fournisseurs.
3. À partir deInformations sur les fournisseurs, choisissez un produit.
4. À partir duSécurité et conformitéonglet, accédez auRésumésection, puis choisissezExporter.
5. Dans la liste déroulante, choisissezTélécharger (JSON)ouTélécharger (CSV).

Contrôle de l'accès dansAWS Marketplace Vendor Insights

AWS Identity and Access Management(IAM) est un outilService AWS qui vous permet de contrôler l'accès auxAWS ressources. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires. Si vous êtes administrateur, vous contrôlez autorisées (disposent d'autorisations) à utiliserAWS Marketplace des ressources. AWS Marketplace Vendor Insights utilise l'IAM pour contrôler l'accès aux données, aux évaluations, à l'auto-attestation du vendeur et aux rapports d'audit standard du secteur.

La méthode recommandée pour contrôler qui peut faire quoiPortail de gestion AWS Marketplace est d'utiliser IAM pour créer des utilisateurs et des groupes. Ensuite, vous devez ajouter les utilisateurs dans des groupes et gérer ces groupes. Vous pouvez affecter au groupe une stratégie ou des autorisations lui accordant un accès en lecture seule. Si d'autres utilisateurs ont besoin d'un accès en lecture seule, vous pouvez les ajouter au groupe que vous avez créé plutôt que d'ajouter des autorisations au leurCompte AWS.

Une stratégie est un document qui définit les autorisations s’appliquant à un utilisateur, un groupe ou un rôle. Les autorisations déterminent ce que les utilisateurs peuvent y faireAWS. Une politique permet généralement d'accéder à des actions spécifiques et peut éventuellement autoriser les actions pour des ressources spécifiques, telles que les instances Amazon EC2, les compartiments Amazon S3, etc. Les stratégies peuvent aussi refuser explicitement l'accès. Une autorisation est une instruction qui accorde ou refuse l'accès à une ressource en particulier ; elle est contenue dans une stratégie.

> **Important**
>
> Tous les utilisateurs que vous créez s'authentifient à l'aide de leurs informations d'identification. Cependant, ils utilisent la même choseCompte AWS. Toute modification apportée par un utilisateur peuvent avoir un impact sur l'ensemble du compte.

AWS Marketplace dispose des autorisations définies pour contrôler les actions qu'une personne dotées de ces autorisations peut effectuer dans Portail de gestion AWS Marketplace. Il existe également des politiques quiAWS Marketplace créent et gèrent plusieurs autorisations. La stratégie `AWSMarketplaceSellerProductsFullAccess` donne à l'utilisateur un accès complet aux produits dans le Portail de gestion AWS Marketplace.

Pour plus d'informations sur les actions, ressources et clés de condition disponibles, consultez Actions, ressources et clés de condition pour la documentationAWS Marketplace de référence de l'autorisation de service.

Autorisations pour les acheteursAWS Marketplace de Vendor Insights

Vous pouvez utiliser les autorisations suivantes dans les politiques IAM pourAWS Marketplace Vendor Insights. Vous pouvez combiner les autorisations au sein d'une politique IAM unique pour accorder les autorisations souhaitées.

`GetProfileAccessTerms`

`GetProfileAccessTerms`permet aux utilisateurs de récupérer les termes nécessaires pour consulter, accepter et accéder à un profilAWS Marketplace Vendor Insights.

Groupes d'actions :

Ressources requises :`SecurityProfile`.

`ListEntitledSecurityProfiles`

`ListEntitledSecurityProfiles`permet aux utilisateurs de répertorier tous les profils de sécurité qu'ils sont autorisés à lire.

Groupes d'actions : lecture seule, liste seule et lecture-écriture.

Ressources nécessaires :

`ListEntitledSecurityProfileSnapshots`

`ListEntitledSecurityProfileSnapshots`permet aux utilisateurs de répertorier les instantanés du profil de sécurité correspondant à un profil de sécurité qu'ils sont autorisés à lire. `SecurityProfile`.

Groupes d'actions : lecture seule, liste seule et lecture-écriture.

Ressources requises :`SecurityProfile`

`GetEntitledSecurityProfileSnapshot`

`GetEntitledSecurityProfileSnapshot`permet aux utilisateurs d'obtenir les détails d'un instantané de profil de sécurité pour un profil de sécurité qu'ils sont autorisés à lire.

Groupes d'actions :

Ressources requises :`SecurityProfile`

Sécurité sur AWS Marketplace

Nous répertorions les logiciels proposés par des vendeurs de grande qualité et nous travaillons activement au maintien de la qualité de notre sélection. Parce que chaque client est différent, notre objectif est de fournir suffisamment d'informations sur les produits listés AWS Marketplace afin que les clients puissent prendre de bonnes décisions d'achat.

> **Note**
>
> Pour plus d'informations sur la sécurité des produits de données d'AWS Data Exchange, consultez la section Sécurité du guide de l'utilisateur d'AWS Data Exchange.
> Pour plus d'informations sur la sécurité pour les vendeursAWS Marketplace, consultez AWS Marketplacela section Sécurité du Guide du AWS Marketplace vendeur.

Informations sur l'abonné partagées avec les vendeurs

Nous pouvons partager vos coordonnées avec nos vendeurs pour les raisons suivantes :

- S'il leur est nécessaire de fournir une formation à la clientèle et un support technique.
- Pour l'activation du logiciel, la configuration et la personnalisation du contenu.
- Compensez leurs équipes de vente en interne.

Par ailleurs, il se peut que nous partagions des informations telles que le nom de la société, l'adresse complète et les frais d'utilisation avec les vendeurs pour qu'ils rémunèrent leurs équipes commerciales. Nous sommes également susceptibles de partager certaines informations avec des vendeurs pour les aider à évaluer l'efficacité de leurs campagnes marketing. Les vendeurs peuvent utiliser ces informations, ainsi que d'autres qui sont déjà en leur possession, pour déterminer la compensation de leurs équipes commerciales ou l'utilisation pour un acheteur spécifique.

Autrement, nous ne partageons généralement aucune information sur le client avec les vendeurs, et toutes les informations partagées ne sont pas identifiables individuellement, à moins que i) vous ayez autorisé le partage de ces informations ; ou ii) nous pensons que ces informations doivent être communiquées aux vendeurs à des fins de conformité avec les lois et règlements.

Mise à niveau des politiques IAM vers IPv6

AWS Marketplaceles clients utilisent des politiques IAM pour définir une plage d'adresses IP autorisée et empêcher toute adresse IP située en dehors de la plage configurée d'accéder auxAWS Marketplace ressources.

Le domaine duAWS Marketplace site Web est en cours de mise à niveau vers le protocole IPv6.

En cas d'absence mise à jour pour gérer le filtrageAWS Marketplace IPv6.

Clients concernés par la mise à niveau IPv4 vers IPv6

Les clients qui utilisent le double adressage sont concernés par cette mise à niveau. Le Dual-Adresh Management signifie que le réseau prend en charge IPv4 et IPv6.

Si vous utilisez le double adressage, vous devez mettre à jour vos politiques IAM actuellement configurées avec des adresses au format IPv4 pour inclure des adresses au format IPv6.

Pour obtenir de l'aide concernant les problèmes d'accès, contactez AWS Support.

> **Note**
>
> Les clients suivants ne sont pas concernés par cette mise à niveau :
>
> - Les clients qui utilisent uniquement des réseaux IPv4.
> - Les clients qui se trouvent uniquement sur des réseaux IPv6.

Qu'est-ce que IPv6 ?

IPv6 est la norme IP de nouvelle génération destinée à remplacer à terme IPv4. La version précédente, IPv4, utilisait un schéma d'adressage 32 bits pour prendre en charge 4,3 milliards d'appareils. IPv6 utilise plutôt un adressage 128 bits pour prendre en charge environ 340 milliards de milliards de milliards de milliards d'appareils (soit 2 pour la 128e puissance).

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

Mise à jour d'une politique IAM pour IPv6

Les politiques IAM sont actuellement utilisées pour définir une plage d'adresses IP autorisée à l'aide du`aws:SourceIp` filtre.

Le double adressage prend en charge le trafic IPv4 et IPV6. Si votre réseau utilise le Dual-Adresh Management Service

Par exemple, cette politique de compartiment Amazon S3 identifie les plages d'adresses IPv4 autorisées`192.0.2.0.*` et`203.0.113.0.*` dans l'`Condition`élément.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

Pour mettre à jour cette politique, l'`Condition`élément de la stratégie est mis à jour pour inclure les plages d'adresses IPv6`2001:DB8:1234:5678::/64` et`2001:cdba:3257:8593::/64`.

> **Note**
>
> NE SUPPRIMEZ PAS les adresses IPv4 existantes car elles sont nécessaires à des fins de rétrocompatibilité.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

Pour plus d'informations sur la gestion des autorisations d'accès avec IAM, consultez la section Politiques gérées et politiques intégrées dans le Guide deAWS Identity and Access Management l'utilisateur.

Test réseau après mise à jour IPv4 vers IPv6

Après avoir mis à jour vos politiques IAM au format IPv6, vous pouvez vérifier si votre réseau accède au point de terminaison IPv6 et aux fonctionnalités duAWS Marketplace site Web.

Rubriques

- Tester le réseau avec Linux/Unix ou Mac OS X
- Tester le réseau avec Windows 7 ou Windows 10
- Tester leAWS Marketplace site Web

Tester le réseau avec Linux/Unix ou Mac OS X

Si vous utilisez Linux/Unix ou Mac OS X, vous pouvez vérifier s'il vous est possible d'accéder au point de terminaison IPv6 à l'aide de la commande curl suivante.

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

Par exemple, si vous êtes connecté via IPv6, l'adresse IP connectée affiche les informations suivantes.

```
* About to connect() to aws.amazon.com port 443 (#0)
*   Trying IPv6 address... connected
* Connected to aws.amazon.com (IPv6 address) port 443 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1 OpenSSL/1.0.1t
 zlib/1.2.3
> Host: aws.amazon.com
```

Tester le réseau avec Windows 7 ou Windows 10

Si vous utilisez Windows 7 ou Windows 10, vous pouvez vérifier s'il vous est possible d'accéder à un point de terminaison Dual-Stack via IPv6 ou IPv4. Utilisez la commande `ping`, comme illustré dans l'exemple suivant.

```
ping aws.amazon.com
```

Cette commande renvoie des adresses IPv6 si vous accédez à un point de terminaison via IPv6.

Tester leAWS Marketplace site Web

Le test des fonctionnalités duAWS Marketplace site Web après la mise à jour dépend principalement de la manière dont votre politique est rédigée et de son utilisation. En général, vous devez vérifier que les fonctionnalités spécifiées dans la politique fonctionnent comme prévu.

Les scénarios suivants vous aident à vérifier les fonctionnalités duAWS Marketplace site Web.

En tant qu'acheteur sur leAWS Marketplace site Web, vérifiez s'il vous est possible d'effectuer les tâches suivantes :

- Abonnez-vous à unAWS Marketplace produit.

- Configurez unAWS Marketplace produit.
- Lancer ou commercialiser unAWS Marketplace produit.

En tant que vendeur sur leAWS Marketplace site Web, vérifiez s'il vous est possible d'effectuer les tâches suivantes :

- Gérez vosAWS Marketplace produits existants.
- Créez unAWS Marketplace produit.

Contrôle de l'accès aux abonnements à AWS Marketplace

AWS IAM Identity Centervous permet de créer ou de connecter en toute sécurité les identités de vos employés et de gérer leur accès de manière centralisée surComptes AWSet applications. IAM Identity Center est l'approche recommandée pour l'authentification et l'autorisation du personnel dansAWSpour les organisations de toutes tailles et de tous types. Pour obtenir des conseils de configuration supplémentaires, consultez leArchitecture de référence de sécurité AWS.

IAM Identity Center fournit un portail utilisateur sur lequel vos utilisateurs peuvent trouver et accéder aux informations qui leur sont attribuéesCompte AWS, des rôles, des applications cloud et des applications personnalisées au même endroit. IAM Identity Center attribue un accès par authentification unique aux utilisateurs et aux groupes de votre annuaire connecté et utilise des ensembles d'autorisations pour déterminer leur niveau d'accès. Cela active les informations d'identification de sécurité temporaires. Vous pouvez définir leur niveau d'accès en leur attribuant desAWSrôles gérés pourAWS Marketplaceaccès pour déléguer la gestion deAWS Marketplaceabonnements sur l'ensemble de votreAWSorganisation.

Par exemple, le client A assume un rôle par le biais de la fédération avec`ManagedMarketplace_ViewOnly`politique associée au rôle. Cela signifie que le client A ne peut consulter les abonnements que dansAWS Marketplace. Vous pouvez créer un rôle IAM autorisé à consulter les abonnements et à autoriser le client A àassumer ce rôle.

Création de rôles IAM pourAWS Marketplaceaccès

Vous pouvez utiliser des rôles IAM pour déléguer l'accès à vos ressources AWS.

Pour créer des rôles IAM à attribuerAWS Marketplaceautorisations

1. Ouvrez la console IAM.

2. Dans le panneau de navigation, choisissez Roles (Rôles), puis Create role (Créer un rôle).
3. Choisissez votre Compte AWS.
4. À partir deAjouter des autorisations, sélectionnez l'une des politiques suivantes :
   - Pour autoriser uniquement l'affichage des abonnements, mais pas leur modification, choisissezAWSMarketplaceRead-only.
   - Pour autoriser les autorisations d'abonnement et de désinscription, choisissezAWSMarketplaceManageSubscriptions.
   - Pour permettre un contrôle complet de vos abonnements, choisissezAWSMarketplaceFullAccess.
5. Choisissez Suivant.
6. PourNom du rôle, entrez le nom du rôle. Par exemple, `MarketplaceReadOnly` ou `MarketplaceFullAccess`. Puis choisissez Create role (Créer un rôle). Pour plus d'informations, voirCréation de rôles IAM.

> **Note**
>
> L'administrateur du compte spécifié peut accorder l'autorisation d'assumer ce rôle à n'importe quel utilisateur de ce compte.

Répétez les étapes précédentes pour créer d'autres rôles avec différents ensembles d'autorisations afin que chaque personnage utilisateur puisse utiliser le rôle IAM avec des autorisations personnalisées.

Vous n'êtes pas limité aux autorisations des stratégies gérées par AWS qui sont décrites ici. Vous pouvez utiliser IAM pour créer des politiques avec des autorisations personnalisées, puis ajouter ces politiques aux rôles IAM. Pour plus d'informations, voirGestion des politiques IAMetAjouter des autorisations d'identité IAM.

Politiques AWS gérées pour AWS Marketplace

Vous pouvez utiliserAWSpolitiques gérées pour fournir des services de baseAWS Marketplaceautorisations. Ensuite, pour chaque scénario unique, vous pouvez créer vos propres politiques et les appliquer aux rôles en fonction des exigences spécifiques de votre scénario.

Les stratégies gérées AWS Marketplace de base suivantes sont disponibles pour contrôler qui dispose des autorisations :

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

AWS Marketplacefournit également des politiques gérées spécialisées pour des scénarios spécifiques. Pour obtenir la liste complète des politiques gérées par AWS pourAWS Marketplaceacheteurs, ainsi que les descriptions des autorisations qu'ils fournissent, voirAWSpolitiques gérées pour les AWS Marketplace acheteurs.

Autorisations pour travailler avec le gestionnaire de licences

AWS Marketplaces'intègre àAWS License Managerpour gérer et partager les licences des produits auxquels vous êtes abonné entre les comptes de votre organisation. Pour consulter tous les détails de vos abonnements dansAWS Marketplace, un utilisateur doit être en mesure de répertorier les informations de licence provenant deAWS License Manager.

Pour vous assurer que vos utilisateurs disposent des autorisations nécessaires pour accéder à toutes les données les concernantAWS Marketplaceproduits et abonnements, ajoutez l'autorisation suivante :

- `license-manager:ListReceivedLicenses`

Pour plus d'informations sur la définition des autorisations, voirGestion des politiques IAMdans leGuide de l'utilisateur IAM.

Ressources supplémentaires

Pour plus d'informations sur la gestion des rôles IAM, voirIdentités IAM (utilisateurs, groupes d'utilisateurs et rôles)dans leGuide de l'utilisateur IAM.

Pour plus d'informations sur la gestion des autorisations et des politiques IAM, voirContrôle de l'accès àAWSressources utilisant des politiquesdans leGuide de l'utilisateur IAM.

Pour plus d'informations sur la gestion des autorisations et des politiques IAM pour les produits de données dans AWS Data Exchange, consultezGestion des identités et des accès dans AWS Data Exchangedans leGuide de l'utilisateur d'AWS Data Exchange.

AWSpolitiques gérées pour les AWS Marketplace acheteurs

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 spécifiques 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 Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Cette section répertorie chacune des politiques utilisées pour gérer l'accès des acheteurs àAWS Marketplace. Pour plus d'informations sur les politiques relatives aux vendeurs, consultez la section Politiques AWS gérées pour AWS Marketplace les vendeurs dans le Guide du AWS Marketplace vendeur.

Rubriques

- AWS Politique gérée par: AWSMarketplaceDeploymentServiceRolePolicy
- Stratégie AWS gérée : AWSMarketplaceFullAccess
- AWSpolitique gérée : AWSMarketplaceImageBuildFullAccess
- AWSpolitique gérée : AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSpolitique gérée : AWSMarketplaceManageSubscriptions
- AWSpolitique gérée : AWSMarketplaceProcurementSystemAdminFullAccess
- AWSpolitique gérée : AWSMarketplaceRead -only

- AWSpolitique gérée : AWSPrivateMarketplaceAdminFullAccess
- AWSpolitique gérée : AWSPrivateMarketplaceRequests
- AWS Politique gérée par: AWSServiceRoleForPrivateMarketplaceAdminPolicy
- Stratégie AWS gérée : AWSVendorInsightsAssessorFullAccess
- Stratégie AWS gérée : AWSVendorInsightsAssessorReadOnly
- Mises à jour AWS Marketplace vers des politiques gérées par AWS

AWS Politique gérée par: AWSMarketplaceDeploymentServiceRolePolicy

Vous ne pouvez pas joindre de `AWSMarketplaceDeploymentServiceRolePolicy` à vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à AWS Marketplace d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AWS Marketplace.

Cette politique accorde aux contributeurs des autorisations leur permettant AWS Marketplace de gérer les paramètres liés au déploiement, qui sont stockés en tant que secrets dans AWS Secrets Manager, en votre nom.

Stratégie AWS gérée : AWSMarketplaceFullAccess

Vous pouvez associer la politique `AWSMarketplaceFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet aux AWS Marketplace services connexes, à la fois en tant qu'acheteur et en tant que vendeur. Ces autorisations incluent la possibilité de s'abonner et de se désinscrire à un AWS Marketplace AWS Marketplace logiciel, de gérer des instances logicielles depuis leAWS Marketplace, de créer et de gérer un marché privé sur votre compte, ainsi que l'accès à Amazon EC2 et Amazon EC2 Systems Manager. AWS CloudFormation

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:*",
                "cloudformation:CreateStack",
```

```
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks",
                "cloudformation:List*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:DeregisterImage",
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:DescribeInstanceStatus",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:CreateTopic",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:setTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*image-build*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        }
    ]
}
```

AWSpolitique gérée : AWSMarketplaceImageBuildFullAccess

> **Important**
>
> AWS Marketplacemettra fin à la méthode de livraison Private Image Build en avril 2024. Le mode de livraison n'est disponible que pour les abonnés existants jusqu'à ce qu'il soit interrompu. Pour plus d'informations, voir Création d'images privées.

Vous pouvez associer la politique `AWSMarketplaceImageBuildFullAccess` à vos identités IAM.

Cette politique accorde aux contributeurs des autorisations permettant un accès complet à la fonctionnalité de création d'images AWS Marketplace privées. Outre la création d'images privées, il fournit également des autorisations pour ajouter des balises aux images, ainsi que pour lancer et mettre fin à des instances Amazon EC2.

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:StartBuild",
                "aws-marketplace:DescribeBuilds"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/marketplace-image-build:build-id": "*"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/*Automation*",
                "arn:aws:iam::*:role/*Instance*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "ec2:DeregisterImage",
                "ec2:CopyImage",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:RunInstances",
                "ec2:DescribeInstanceStatus",
                "sns:GetTopicAttributes",
                "iam:GetRole",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
```

```
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*image-build*"
            ]
        }
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/marketplace-image-build:build-id": "*"
                },
                "StringNotEquals": {
                    "ec2:CreateAction": "RunInstances"
                }
            }
        }
    ]
}
```

AWSpolitique gérée : AWSMarketplaceLicenseManagementServiceRolePolicy

Vous ne pouvez pas vous associer AWSMarketplaceLicenseManagementServiceRolePolicy à vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à AWS Marketplace d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AWS Marketplace.

Cette politique accorde aux contributeurs des autorisations leur AWS Marketplace permettant de gérer les licences en votre nom.

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLicenseManagerActions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "license-manager:ListReceivedGrants",
                "license-manager:ListDistributedGrants",
                "license-manager:GetGrant",
                "license-manager:CreateGrant",
                "license-manager:CreateGrantVersion",
                "license-manager:DeleteGrant",
                "license-manager:AcceptGrant"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWSpolitique gérée : AWSMarketplaceManageSubscriptions

Vous pouvez associer la politique `AWSMarketplaceManageSubscriptions` à vos identités IAM.

Cette politique accorde aux contributeurs des autorisations leur permettant de s'abonner ou de se désinscrire à des produits. AWS Marketplace

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "aws-marketplace:Subscribe",
                "aws-marketplace:Unsubscribe"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWSpolitique gérée : AWSMarketplaceProcurementSystemAdminFullAccess

Vous pouvez associer la politique `AWSMarketplaceProcurementSystemAdminFullAccess` à vos identités IAM.

Cette politique accorde des autorisations d'administrateur qui permettent de gérer tous les aspects d'une intégration d'AWS Marketplaceachats électroniques, y compris la liste des comptes de

votre organisation. Pour plus d'informations sur les intégrations d'achats électroniques, consultez. Intégration de AWS Marketplace à des systèmes d'approvisionnement

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:PutProcurementSystemConfiguration",
                "aws-marketplace:DescribeProcurementSystemConfiguration",
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWSpolitique gérée : AWSMarketplaceRead -only

Vous pouvez associer la politique `AWSMarketplaceRead-only` à vos identités IAM.

Cette politique accorde des autorisations en lecture seule qui permettent de consulter les produits, les offres privées et les abonnements associés à votre compte surAWS Marketplace, ainsi que de consulter les ressources Amazon EC2 AWS Identity and Access Management et Amazon SNS du compte.

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
```

```
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:DescribeBuilds",
                "iam:ListRoles",
                "iam:ListInstanceProfiles",
                "sns:GetTopicAttributes",
                "sns:ListTopics"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWSpolitique gérée : AWSPrivateMarketplaceAdminFullAccess

Vous pouvez associer la politique `AWSPrivateMarketplaceAdminFullAccess` à vos identités IAM.

Cette politique accorde des autorisations d'administrateur qui permettent un accès complet à la gestion des marchés privés de votre compte (ou de votre organisation). Pour plus d'informations sur l'utilisation de plusieurs administrateurs, consultezthe section called “Création de politiques personnalisées pour les administrateurs de marchés privés”.

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceRequestPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:StartChangeSet",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogTaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:TagResource",
                "aws-marketplace:UntagResource",
                "aws-marketplace:ListTagsForResource"
```

```
            ],
            "Resource": "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSpolitique gérée : AWSPrivateMarketplaceRequests

Vous pouvez associer la politique `AWSPrivateMarketplaceRequests` à vos identités IAM.

Cette politique accorde aux contributeurs des autorisations leur permettant de demander l'ajout de produits à votre place de marché privée et de consulter ces demandes. Ces demandes doivent être approuvées ou refusées par un administrateur du marché privé.

Détails des autorisations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
```

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

AWS Politique gérée par: AWSServiceRoleForPrivateMarketplaceAdminPolicy

Vous ne pouvez pas joindre de `AWSServiceRoleForPrivateMarketplaceAdminPolicy` à vos entités IAM. Cette politique est attachée à un rôle lié au service qui permet à AWS Marketplace d'effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AWS Marketplace.

Cette politique accorde aux contributeurs des autorisations leur permettant de décrire et de mettre AWS Marketplace à jour les ressources de Private Marketplace et de les décrireAWS Organizations.

Stratégie AWS gérée : AWSVendorInsightsAssessorFullAccess

Vous pouvez associer la politique `AWSVendorInsightsAssessorFullAccess` à vos identités IAM.

Cette politique accorde un accès complet à la consultation des ressources intitulées AWS Marketplace Vendor Insights et à la gestion des abonnements AWS Marketplace Vendor Insights. Ces demandes doivent être approuvées ou refusées par un administrateur. Il permet un accès en lecture seule aux rapports AWS Artifact tiers.

AWS MarketplaceVendor Insights identifie que l'évaluateur est égal à l'acheteur et le fournisseur est égal au vendeur.

Détails des autorisations

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
```

```
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:AgreementType": "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Stratégie AWS gérée : AWSVendorInsightsAssessorReadOnly

Vous pouvez associer la politique `AWSVendorInsightsAssessorReadOnly` à vos identités IAM.

Cette politique accorde un accès en lecture seule pour consulter les ressources intitulées AWS Marketplace Vendor Insights. Ces demandes doivent être approuvées ou refusées par un administrateur. Il permet un accès en lecture seule aux rapports dans. AWS Artifact

les demandes doivent être approuvées ou refusées par un administrateur. Il permet un accès en lecture seule aux rapports AWS Artifact tiers.

AWS MarketplaceVendor Insights identifie l'évaluateur comme l'acheteur et le vendeur est égal au vendeur aux fins de ce guide.

Détails des autorisations

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Mises à jour AWS Marketplace vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS Marketplace depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page AWS Marketplace Historique du document.

Modification	Description	Date
AWSServiceRoleForPrivateMarketplaceAdminPolicy— Ajout d'une politique pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplacea ajouté une nouvelle politique pour soutenir la gestion des ressources du Private Marketplace et les décrireAWS Organizations.	16 février 2024
AWSPrivateMarketplaceAdminFullAccess – Mise à jour de la politique existante	AWS Marketplacea mis à jour la politique pour soutenir la lecture AWS Organizations des données.	16 février 2024
AWSMarketplaceDeploymentServiceRolePolicy— Ajout d'une politique pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplacea ajouté une nouvelle politique pour prendre en charge la gestion des paramètres liés au déploiement.	29 novembre 2023
AWSMarketplaceRead-uniquement et AWSMarketplaceManageSubscriptions— mises à jour des politiques existantes	AWS Marketplacea mis à jour les politiques existantes pour autoriser l'accès à la page des offres privées.	19 janvier 2023
AWSPrivateMarketplaceAdminFullAccess – Mise à jour de la politique existante	AWS Marketplacea mis à jour la politique relative à la nouvelle fonctionnalité d'autorisation basée sur des balises.	9 décembre 2022
AWSVendorInsightsAssessorReadOnlyAWS Marketplacemis à jour `AWSVendorInsightsAssessorReadOnly`	AWS Marketplacemis `AWSVendorInsightsAssessorReadOnly` à jour pour ajouter un accès en lecture seule aux rapports	30 novembre 2022

Modification	Description	Date
	d'un rapport AWS Artifact tiers (version préliminaire).	
AWSVendor InsightsAssessorFu llAccessAWS Marketpla cemis à jour `AWSVendor InsightsAssessorFu llAccess`	AWS Marketplacemis `AWSVendorInsightsA ssessorFullAccess` à jour pour ajouter la recherche d'accords et l'accès en lecture seule au rapport AWS Artifact tiers (aperçu).	30 novembre 2022
AWSVendorInsightsA ssessorFullAccessetAWSVendorInsightsA ssessorReadOnly— Ajout de politiques pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplacepolitiques ajoutées pour la nouvelle fonctionnalité AWS Marketpla ce Vendor Insights : `AWSVendorInsightsA ssessorFullAccess` et `AWSVendorInsightsA ssessorReadOnly`	26 juillet 2022
AWSMarketplaceFullAccessetAWSMarketplaceImag eBuildFullAccess— Mises à jour d'une politique existante	AWS Marketplacea supprimé les autorisations qui ne sont plus nécessaires pour améliorer la sécurité.	4 mars 2022
AWSPrivateMarketpl aceAdminFullAccess - mise à jour d'une politique existante	AWS Marketplacea supprimé les autorisations non utilisées dans la `AWSPrivat eMarketplaceAdminF ullAccess` politique.	27 août 2021

Modification	Description	Date
AWSMarketplaceFullAccess - mise à jour d'une politique existante	AWS Marketplacea supprimé une `ec2:DescribeAccountAttributes` autorisation dupliquée de `AWSMarketplaceFullAccess` la politique.	20 juillet 2021
AWS Marketplace a démarré le suivi des modifications	AWS Marketplace a commencé à suivre les modifications pour ses politiques gérées par AWS.	20 avril 2021

Trouver votreCompte AWS numéro pour le service client

Si vous ou vos utilisateurs avez besoin de nous contacterAWS Support, vous avez besoin de votreCompte AWS numéro.

Pour trouver votreCompte AWS numéro

1. Connectez-vous à l'AWS Management Consoleaide de votre nom d'utilisateur.
2. Dans la barre de navigation supérieure, choisissez Support, puis Centre de support.

VotreCompte AWS identifiant (numéro de compte) apparaît sous la barre de navigation supérieure.

Utilisation des rôles liés aux services pour AWS Marketplace

AWS Marketplace utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Marketplace. Les rôles liés à un service sont prédéfinis par AWS Marketplace et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Rubriques

- Utiliser des rôles pour partager des droits pour AWS Marketplace
- Utilisation des rôles pour traiter les bons de commande dans AWS Marketplace

- Utilisation de rôles pour configurer et lancer des produits dans AWS Marketplace
- Utiliser des rôles pour configurer Private Marketplace dans AWS Marketplace

Utiliser des rôles pour partager des droits pour AWS Marketplace

AWS Marketplace utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Marketplace. Les rôles liés à un service sont prédéfinis par AWS Marketplace et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service facilite la configuration AWS Marketplace car il n'est pas nécessaire d'ajouter les autorisations nécessaires manuellement. AWS Marketplacedéfinit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Marketplace peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Cette politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Pour partager vos AWS Marketplace abonnements à d'autres comptes de votre AWS organisationAWS License Manager, vous devez accorder AWS Marketplace des autorisations pour chaque compte avec lequel vous souhaitez partager. Pour ce faire, utilisez le AWSServiceRoleForMarketplaceLicenseManagementrôle. Pour plus d’informations, consultez Création d'un rôle lié à un service pour AWS Marketplace.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWSServices qui fonctionnent avec IAM et recherchez les services marqués Oui dans la colonne Rôles liés à un service. Cliquez sur Oui avec un lien pour consulter la documentation relative aux rôles liés à un service pour ce service.

Autorisations des rôles liés à un service pour AWS Marketplace

AWS Marketplace utilise le rôle lié à un service AWSServiceRoleForMarketplaceLicenseManagement. Ce rôle fournit AWS Marketplace des autorisations pour créer et gérer des licences AWS License Manager pour les produits auxquels vous êtes abonnéAWS Marketplace.

Le rôle AWSServiceRoleForMarketplaceLicenseManagementlié à un service fait confiance au service suivant pour effectuer des actions dans License Manager en votre nom :

- `license-management.marketplace.amazonaws.com`

La politique d'autorisations de rôle nommée AWSMarketplaceLicenseManagementServiceRolePolicyAWS Marketplacepermet d'effectuer les actions suivantes sur les ressources spécifiées :

- Actions:
  - `"organizations:DescribeOrganization"`
  - `"license-manager:ListReceivedGrants"`
  - `"license-manager:ListDistributedGrants"`
  - `"license-manager:GetGrant"`
  - `"license-manager:CreateGrant"`
  - `"license-manager:CreateGrantVersion"`
  - `"license-manager:DeleteGrant"`
  - `"license-manager:AcceptGrant"`
- Ressources :
  - Toutes les ressources (`"*"`)

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Marketplace

AWS Marketplacecrée pour vous le rôle lié au service lorsque vous configurez l'intégration avec. AWS License Manager

Vous pouvez spécifier de AWS Marketplace créer le rôle lié au service pour tous les comptes de votre organisation en une seule fois, ou vous pouvez créer le rôle lié au service pour un compte à la fois. L'option permettant de créer des rôles liés à un service pour tous les comptes n'est disponible que si toutes les fonctionnalités de votre organisation sont activées. Pour plus de détails, consultez la section Activation de toutes les fonctionnalités de votre organisation dans le guide de AWS Organizations l'utilisateur.

Pour créer des rôles liés à un service sur tous les comptes

1. Dans AWS Marketplacela console, connectez-vous et choisissez Paramètres.

2. Dans la section AWS OrganizationsIntégration, sélectionnez Créer une intégration.
3. Sur la page Créer une AWS Organizations intégration, sélectionnez Activer l'accès sécurisé au sein de votre organisation, puis choisissez Créer une intégration.

> **Note**
>
> Ce paramètre permet d'instaurer la confiance interneAWS Organizations. Par conséquent, en plus de l'action en cours, le rôle lié au service sera automatiquement ajouté aux futurs comptes ajoutés à l'organisation.

Pour créer des rôles liés à un service pour le compte courant

1. Dans AWS Marketplacela console, connectez-vous et choisissez Paramètres.
2. Dans la section AWS OrganizationsIntégration, sélectionnez Configurer l'intégration.
3. Sur la page Créer une AWS Organizations intégration, sélectionnez le rôle lié au service de gestion des AWS Marketplace licences pour ce compte, puis choisissez Créer une intégration.

> **Important**
>
> Si vous choisissez de créer le rôle lié au service uniquement pour le compte courant, cela ne permet pas un accès fiable au sein de votre organisation. Vous devez répéter ces étapes pour chaque compte dans lequel vous souhaitez partager (donner ou recevoir) des licencesAWS Marketplace. Cela inclut les comptes qui seront ajoutés à l'organisation dans le futur.

Modification d'un rôle lié à un service pour AWS Marketplace

AWS Marketplace ne vous permet pas de modifier le rôle lié à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Marketplace

Si vous n’avez plus besoin d’utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n’avez aucune entité inutilisée qui n’est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service AWS Marketplace utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer manuellement le rôle lié à un service à l’aide d’IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForMarketplaceLicenseManagement. Pour plus d’informations, consultez Suppression d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Marketplace

AWS Marketplace prend en charge l’utilisation des rôles liés à un service dans toutes les Régions AWS où le service est disponible. Pour plus d’informations, consultez Régions et Points de terminaison AWS Marketplace.

Utilisation des rôles pour traiter les bons de commande dans AWS Marketplace

AWS Marketplace utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Marketplace. Les rôles liés à un service sont prédéfinis par AWS Marketplace et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service permet d'utiliser AWS Marketplace plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS Marketplace définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul AWS Marketplace peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources AWS Marketplace sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS Marketplace

AWS Marketplaceutilise le rôle lié au service nommé AWSServiceRoleForMarketplacePurchaseOrders: ce rôle permet d'associer AWS Marketplace des numéros de bon de commande à vos AWS Marketplace abonnements dans. AWS Billing and Cost Management

Le rôle lié à un service AWSServiceRoleForMarketplacePurchaseOrders approuve les services suivants pour endosser le rôle :

- `purchase-orders.marketplace.amazonaws.com`

La politique d'autorisations de rôle nommée AWSMarketplacePurchaseOrdersServiceRolePolicyAWS Marketplacepermet d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `"purchase-orders:ViewPurchaseOrders", "purchase-orders:ModifyPurchaseOrders"` sur `"*"`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Marketplace

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous configurez l'intégration avecAWS Billing and Cost Management, AWS Marketplace crée le rôle lié au service pour vous.

> **Note**
>
> Dans ce AWS Organizations cas, ce paramètre ne fonctionne que dans le compte de gestion. Vous devez effectuer cette procédure depuis le compte de gestion. Cela permet de configurer le rôle lié au service et la prise en charge des bons de commande pour tous les comptes de l'organisation.

Pour créer un rôle lié à un service

1. Dans la AWS Marketplaceconsole, connectez-vous au compte de gestion et choisissez Paramètres.
2. Dans la section Intégration AWS de la facturation, sélectionnez Configurer l'intégration.
3. Sur la page Créer une intégration AWS de facturation, sélectionnez le rôle lié au service de gestion de AWS Marketplace facturation pour votre organisation, puis choisissez Créer une intégration.

Si vous supprimez ce rôle lié à un service et que vous devez ensuite le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous configurez l'intégration avecAWS Billing and Cost Management, AWS Marketplace crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Marketplace

AWS Marketplace ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForMarketplacePurchaseOrders. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour en savoir plus, consultez Modification d’un rôle lié à un service dans le guide de l’utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Marketplace

Si vous n’avez plus besoin d’utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Suppression manuelle du rôle lié à un service

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForMarketplacePurchaseOrders. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Marketplace

AWS Marketplace prend en charge l'utilisation des rôles liés à un service dans toutes les Régions AWS où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS Marketplace.

Utilisation de rôles pour configurer et lancer des produits dans AWS Marketplace

AWS Marketplace utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Marketplace. Les rôles liés à un service sont prédéfinis par AWS Marketplace et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service permet d'utiliser AWS Marketplace plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS Marketplace définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul AWS Marketplace peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS Marketplace

AWS Marketplaceutilise le rôle lié au service nommé AWSServiceRoleForMarketplaceDeploymentpour permettre AWS Marketplace de gérer les paramètres liés au déploiement, qui sont stockés en tant que secrets dans AWS Secrets Manager, en votre nom. Ces secrets peuvent être référencés par les vendeurs dans des AWS CloudFormation modèles, que vous pouvez lancer lorsque vous configurez des produits pour lesquels le lancement rapide est activéAWS Marketplace.

Le rôle lié à un service AWSServiceRoleForMarketplaceDeployment approuve les services suivants pour endosser le rôle :

- `deployment.marketplace.amazonaws.com`

Utilisez la politique d'autorisation des rôles nommée AWSMarketplaceDeploymentServiceRolePolicypour AWS Marketplace permettre d'effectuer les actions sur vos ressources.

> **Note**
>
> Pour plus d'informations sur les politiques AWS Marketplace gérées, consultez la section Politiques gérées par AWS pour AWS Marketplace les acheteurs.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ManageMarketplaceDeploymentSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:DeleteSecret",
    "secretsmanager:RemoveRegionsFromReplication"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "ListSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:ListSecrets"
   ],
   "Resource": [
```

```
      "*"
     ]
    },
    {
     "Sid": "TagMarketplaceDeploymentSecrets",
     "Effect": "Allow",
     "Action": [
      "secretsmanager:TagResource"
     ],
     "Resource": "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
     "Condition": {
      "Null": {
       "aws:RequestTag/expirationDate": "false"
      },
      "ForAllValues:StringEquals": {
       "aws:TagKeys": [
        "expirationDate"
       ]
      },
      "StringEquals": {
       "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
     }
    }
   ]
}
```

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Marketplace

La configuration du rôle lié à un service est une action ponctuelle qui fournit les autorisations pour tous les produits pour lesquels le lancement rapide est activé, tant que le rôle existe.

Lorsque vous configurez un produit sur lequel le lancement rapide est activé, il AWS Marketplace détecte si le rôle lié au service requis a été créé pour votre compte. Si le rôle est absent, une invite s'affiche pour activer l'intégration des paramètres de AWS Marketplace déploiement, qui inclut un bouton Activer l'intégration. AWS Marketplacecrée pour vous le rôle lié au service lorsque vous sélectionnez ce bouton.

> **Important**
>
> Ce rôle lié au service apparaîtra dans votre compte si vous avez déjà configuré un produit sur lequel le lancement rapide est activé. Pour plus d'informations, voir Un nouveau rôle est apparu dans mon Compte AWS.

Si vous supprimez ce rôle lié au service et que vous devez le créer à nouveau, vous pouvez utiliser le même processus pour recréer le rôle dans votre compte. Lorsque vous ouvrez la page de configuration d'un produit pour lequel le lancement rapide est activé, vous verrez le bouton Activer l'intégration, que vous pouvez sélectionner à nouveau pour recréer le rôle lié au service.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service selon le cas d'utilisation d'AWS Marketplace - Deployment Management. Dans l'interface AWS CLI ou l'API AWS, créez un rôle lié à un service avec le nom de service `deployment.marketplace.amazonaws.com`. Pour de plus amples informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Marketplace

AWS Marketplacene vous permet pas de modifier le rôle lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Marketplace

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service utilise le rôle lorsque vous essayez de le supprimer, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les AWS Marketplace ressources utilisées par le `deployment.marketplace.amazonaws.com` service, vous devez supprimer tous les secrets relatifs à Marketplace Deployment de. SecretsManager Vous pouvez trouver les secrets pertinents en :

- À la recherche de secrets gérés par`marketplace-deployment`.
- Recherche de secrets à l'aide de la clé `aws:secretsmanager:owningService` et de la valeur du tag`marketplace-deployment`.
- Recherche de secrets dont le nom est préfixé par`marketplace-deployment!`.

Pour supprimer le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForMarketplaceDeployment. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Marketplace

AWS Marketplace prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez la section Régions et points de terminaison AWS Marketplace.

Utiliser des rôles pour configurer Private Marketplace dans AWS Marketplace

AWS Marketplace utilise des rôles AWS Identity and Access Management (IAM) liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à AWS Marketplace. Les rôles liés à un service sont prédéfinis par AWS Marketplace et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service permet d'utiliser AWS Marketplace plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. AWS Marketplace définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul AWS Marketplace peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention

Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS Marketplace

AWS Marketplaceutilise le rôle lié au service nommé AWSServiceRoleForPrivateMarketplaceAdminpour décrire et mettre à jour les ressources de Private Marketplace et pour décrire. AWS Organizations

Le rôle lié à un service AWSServiceRoleForPrivateMarketplaceAdmin approuve les services suivants pour endosser le rôle :

- `private-marketplace.marketplace.amazonaws.com`

Utilisez la politique d'autorisation de rôle nommée AWSServiceRoleForPrivateMarketplaceAdminPolicypour AWS Marketplace permettre d'effectuer les actions suivantes sur des ressources spécifiées.

> **Note**
>
> Pour plus d'informations sur les politiques gérées par AWS Marketplace, consultez la section Politiques gérées par AWS pour AWS Marketplace les acheteurs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceCatalogDescribePermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
            ]
        },
        {
```

```
            "Sid": "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogListPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceStartChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AssociateAudience",
                        "DisassociateAudience"
                    ]
                }
            },
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren"
            ],
```

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Marketplace

Vous n'avez pas besoin de créer manuellement un rôle lié au service . Lorsque vous activez Private Marketplace pour votre organisation, vous AWS Marketplace créez le rôle lié au service pour vous.

> **Note**
>
> Ce rôle est requis uniquement dans le compte de gestion de AWS Organizations et est créé uniquement dans le compte de gestion.

Pour créer un rôle lié à un service

1. Sur la page Getting started with Private Marketplace, sélectionnez les options permettant d'activer un accès sécurisé au sein de votre organisation et créez un rôle lié au service Private Marketplace. Ces options ne sont disponibles que pour le compte de gestion.
2. Choisissez Enable Private Marketplace.

Si vous êtes déjà client de Private Marketplace, les options permettant d'activer un accès fiable au sein de votre organisation et d'activer un rôle lié au service Private Marketplace seront disponibles sur la page Paramètres du tableau de bord administratif de votre place de marché privée.

Si vous supprimez ce rôle lié au service et que vous devez le créer à nouveau, vous pouvez utiliser le même processus pour recréer le rôle dans votre compte.

Modification d'un rôle lié à un service pour AWS Marketplace

AWS Marketplace ne vous permet pas de modifier le rôle lié à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités

peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Marketplace

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

Avant de pouvoir supprimer le rôle lié à un service, vous devez :

- Désactivez l'accès sécurisé au sein de votre organisation.
- Dissociez toutes les expériences du marché privé.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForPrivateMarketplaceAdmin. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Marketplace

AWS Marketplace prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez la section Régions et points de terminaison AWS Marketplace.

Création d'un administrateur de marché privé

Vous pouvez créer un groupe d'administrateurs pour gérer les paramètres du marché privé de votre entreprise. Une fois le marché privé activé pour votre organisation, les administrateurs du marché privé peuvent effectuer de nombreuses tâches, notamment les suivantes :

- Visualisez et créez des expériences et des audiences.
- Ajoutez des produits aux expériences des marchés privés.
- Supprimez les produits des expériences des marchés privés.

- Configurez l'interface utilisateur des expériences de marché privées.
- Activez et désactivez les expériences de marché privées.
- Appelez-le AWS Marketplace Catalog API pour gérer les expériences des marchés privés de manière programmatique.

Pour créer plusieurs administrateurs de marchés privés, chaque administrateur étant limité à un sous-ensemble de tâches, voirthe section called “Création de politiques personnalisées pour les administrateurs de marchés privés”.

> **Note**
>
> L'activation du marché privé est une action ponctuelle qui doit être effectuée à partir du compte de gestion. Pour plus d'informations, consultez Commencer à utiliser un marché privé.

Vous accordez des autorisations AWS Identity and Access Management (IAM) pour administrer votre place de marché privée en l'associant the section called “AWSPrivateMarketplaceAdminFullAccess” à un utilisateur, à un groupe ou à un rôle. Nous vous recommandons d'utiliser un groupe ou un rôle. Pour plus d'informations sur la manière d'associer la politique, consultez la section Attacher une politique à un groupe d'utilisateurs dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations définies dans la `AWSPrivateMarketplaceAdminFullAccess` politique, consultezthe section called “AWSPrivateMarketplaceAdminFullAccess”. Pour en savoir plus sur les autres politiques à utiliserAWS Marketplace, connectez-vous auAWS Management Console, puis rendez-vous sur la page des politiques IAM. Dans le champ de recherche, entrez **`Marketplace`** pour trouver toutes les politiques associées àAWS Marketplace.

Création de politiques personnalisées pour les administrateurs de marchés privés

Votre organisation peut créer plusieurs administrateurs du marché privé, chaque administrateur étant limité à un sous-ensemble de tâches. Vous pouvez ajuster les politiques AWS Identity and Access Management (IAM) pour spécifier des clés de condition et des ressources pour les AWS Marketplace Catalog API actions répertoriées dans Actions, ressources et clés de condition pour AWS Marketplace Catalog. Le mécanisme général d'utilisation des types de AWS Marketplace

Catalog API modification et des ressources pour ajuster les politiques IAM est décrit dans le guide de l'API AWS Marketplace Catalog. Pour obtenir la liste de tous les types de modifications disponibles dans le mode privéAWS Marketplace, consultez la section Utilisation d'un marché privé.

Pour créer des politiques gérées par le client, consultez la section Création de politiques IAM. Vous trouverez ci-dessous un exemple de politique JSON que vous pouvez utiliser pour créer un administrateur qui peut uniquement ajouter ou supprimer des produits sur des sites de vente privés.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AllowProductProcurement",
```

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

Une politique peut également être limitée pour gérer un sous-ensemble de ressources du marché privé. Voici un exemple de politique JSON que vous pouvez utiliser pour créer un administrateur qui ne peut gérer qu'une expérience de marché privée spécifique. Cet exemple utilise une chaîne de ressource ayant `exp-1234example` comme `Experience` identifiant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "aws-marketplace:StartChangeSet"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/exp-1234example"
            ]
        }
    ]
}
```

Pour plus de détails sur la manière dont les identifiants d'entité peuvent être récupérés et pour consulter l'ensemble des ressources du marché privé, voir Travailler avec un marché privé.

Historique du document

Le tableau suivant décrit la documentation de cette version du Guide de l'AWS Marketplaceacheteur.

Pour être informé des mises à jour de cette documentation, vous pouvez vous abonner au flux RSS.

Modification	Description	Date
Politique de AWS Organizations support mise à jour	Politique gérée mise à jour `AWSPrivateMarketplaceAdminFullAccess` pour autoriser l'accès aux AWS Organizations données en lecture.	16 février 2024
Nouveau rôle lié au service pour les produits dans AWS Marketplace	AWS Marketplacefournit désormais un rôle lié à un service pour décrire et mettre à jour les ressources de Private Marketplace et les décrire. AWS Organizations	16 février 2024
Nouvelle expérience de marché privé sur AWS Marketplace	AWS Marketplaceprend désormais en charge l'intégration AWS Organizations et la possibilité d'enregistrer des administrateurs délégués pour administrer les expériences du marché privé.	16 février 2024
Disponibilité générale pour les futurs contrats datés en AWS Marketplace	La fonctionnalité des contrats à date future pour tous les ISV et partenaires de distribution du SaaS est désormais généralement disponible dansAWS Marketplace. En utilisant des contrats à date	16 janvier 2024

	future, les clients peuvent réserver à l'avance des offres ou configurer des renouvell ements lorsqu'ils ont déjà acheté des produits sur la même liste de produits, avec un effort opérationnel réduit.	
Support pour la région du Canada Ouest (Calgary)	AWS Marketplaceprend désormais en charge ce qui suit Région AWS : Canada West (Calgary).	20 décembre 2023
Nouveau rôle lié au service pour les produits dans AWS Marketplace	AWS Marketplacefournit désormais un rôle lié au service pour gérer les paramètres liés au déploieme nt, qui sont stockés sous forme de secrets pour le compte des AWS Secrets Manager acheteurs.	29 novembre 2023
Nouvelle option de déploieme nt de Quick Launch pour les acheteurs	Les acheteurs peuvent désormais réduire le temps, les ressources et les étapes nécessaires pour configure r, déployer et lancer les produits SaaS applicables dansAWS Marketplace.	29 novembre 2023
Des calendriers de paiement flexibles sont disponibles pour les offres privées	Les calendriers de paiement flexibles (FPS) pour les offres privées sont désormais disponibles pour tous les clients duAWS Marketplace.	17 novembre 2023

Extensions tierces d'Amazon EKS	Les clients peuvent désormais s'abonner à des modules complémentaires tiers depuis la console Amazon EKS sans être redirigés versAWS Marketplace.	18 octobre 2023
Support pour Amazon EventBridge	AWS Marketplaceest désormais intégré à Amazon EventBridge, anciennement Amazon CloudWatch Events.	6 septembre 2023
Support à la région d'Israël (Tel Aviv)	AWS Marketplacesoutient désormais ce qui suit Région AWS : Israël (Tel Aviv).	1er août 2023
Assistance aux bons de commande pour les contrats annuels AMI	AWS Marketplaceprend désormais en charge la fonctionnalité de commande pour les contrats annuels Amazon Machine Image (AMI).	29 juin 2023
Disponibilité des bons de commande dans AWS Billing la console	Les acheteurs peuvent désormais gérer tous leurs bons de commande dans la AWS Billing console et concilier facilement les factures PDF de leurs contrats out-of-cycle SaaS avec les bons de commande correspon dants.	3 février 2023

Support pour la région Asie-Pacifique (Melbourne)	AWS Marketplaceprend désormais en charge les éléments suivants Région AWS : Asie-Pacifique (Melbourne).	24 janvier 2023
Page des politiques mises à jour pour les offres privées	Politiques gérées mises `AWSMarketplaceManageSubscriptions` à jour `AWSMarketplaceRead-only` et autorisation d'accès à la page des offres privées.	19 janvier 2023
Page d'offres privées	Les acheteurs authentifiés peuvent désormais consulter les offres AWS Marketplace privées qui leur sont proposées Compte AWS sur la page des offres privées.	19 janvier 2023
Notifications par e-mail mises à jour pour les acheteurs	Les acheteurs sont désormais avertis lorsqu'une offre privée est publiée.	22 décembre 2022
Les essais gratuits du SaaS pour les abonnements sont désormais disponibles pour les acheteurs sur AWS Marketplace	Les acheteurs peuvent désormais s'abonner à des essais gratuits pour les produits SaaS par abonnement.	16 décembre 2022
Les acheteurs peuvent accepter une mise à niveau ou un renouvellement d'une offre privée SaaS	Si un vendeur a amélioré ou renouvelé une offre privée SaaS précédente, les acheteurs peuvent accepter une nouvelle offre privée sans avoir à annuler leur contrat existant.	13 décembre 2022

AWS Marketplaceprend en charge l'archivage des expériences des marchés privés	Les acheteurs peuvent désormais archiver et réactiver les expériences des marchés privés dansAWS Marketplace.	12 décembre 2022
Politique mise à jour pour la fonctionnalité d'autorisation AWS Marketplace basée sur des balises	Mise à jour de la `AWSPrivateMarketplaceAdminFullAccess` politique pour prendre en charge l'autorisation basée sur des balises dansAWS Marketplace.	9 décembre 2022
Ajout d'une nouvelle rubrique fournissant des informations sur la façon d'annuler votre abonnement	Ajout d'informations sur la manière d'annuler votre abonnement aux produits AMI, ML et SaaS dansAWS Marketplace. Nous avons également ajouté des informations sur l'annulation du renouvellement automatique d'un contrat SaaS.	8 décembre 2022
Politiques mises à jour pour les acheteurs dans AWS Marketplace Vendor Insights	Politiques gérées mises à jour `AWSVendorInsightsAssessorFullAccess` et `AWSVendorInsightsAssessorReadOnly` pour les acheteurs de AWS Marketplace Vendor Insights.	30 novembre 2022
Contrôle de l'accès des acheteurs dans AWS Marketplace Vendor Insights	Ajout d'une nouvelle rubrique dans AWS Marketplace Vendor Insights pour décrire les actions et les autorisations disponibles pour les acheteurs .	30 novembre 2022

Support pour la région Asie-Pacifique (Hyderabad)	AWS Marketplaceprend désormais en charge les systèmes suivants Région AWS : Asie-Pacifique (Hyderabad).	22 novembre 2022
Support pour la région Europe (Espagne)	AWS Marketplaceprend désormais en charge les éléments suivants Région AWS : Europe (Espagne).	16 novembre 2022
Support pour la région Europe (Zurich)	AWS Marketplaceprend désormais en charge les éléments suivants Région AWS : Europe (Zurich).	9 novembre 2022
AWS Marketplacemise à niveau du site Web vers IPv6 d'ici décembre 2022	Les acheteurs qui utilisent actuellement l'adresse au format IPv4 dans leurs politiques IAM sont invités à mettre à jour leurs politique s IAM vers des adresses au format IPv6 avant le 15 décembre 2022.	29 septembre 2022
AWS MarketplaceAutoris ations granulaires sur le marché privé	Les acheteurs disposent désormais d'autorisations plus précises pour gérer les expériences des marchés privés.	8 septembre 2022

Ajout de deux politiques pour AWS Marketplace Vendor Insights.	Ajout de deux politiques `AWSVendorInsightsAssessorFullAccess` et, `AWSVendorInsightsAssessorReadOnly` pour AWS Marketplace Vendor Insights, d'une fonctionnalité proposant une évaluation des risques logiciels.	26 juillet 2022
Informations sur les fournisseurs AWS Marketplace	AWS MarketplaceVendor Insights est une fonctionnalité proposant une évaluation des risques logiciels.	26 juillet 2022
Mise à jour des méthodes de paiement	Mise à jour basée uniquement sur la documentation pour clarifier comment modifier les modes de paiement dans la console de AWS facturation.	1 juin 2022
Essais gratuits de SaaS pour les contrats	Les acheteurs peuvent désormais s'abonner à des essais gratuits de SaaS pour des contrats visant à explorer des produits avant de passer à des essais payants.	31 mai 2022
Des balises de mesure du fournisseur ont été ajoutées pour les produits AMI, Container et SaaS	Nouvelle fonctionnalité fournissant des balises pour aider les clients à comprendre leur utilisation AWS Marketplace des ressources selon les indicateurs fournis par le fournisseur.	27 mai 2022

Notifications par e-mail ajoutées aux transactions des acheteurs	Nouvelle fonctionnalité permettant d'envoyer des notifications par e-mail à l'acheteur pour vérifier les accords conclusAWS Marketplace.	23 mai 2022
L'approbation automatique des produits Free/BYOL pour les clients d'eProcurement est activée	Les clients peuvent utiliser les produits immédiatement grâce à la nouvelle approbation automatique des produits Free/BYOL pour les clients d'eProcurement.	2 mai 2022
Modifications de contrat activées pour les acheteurs dans les contrats AMI et Container Product	Les contrats relatifs aux produits AMI et Container peuvent être modifiés pour acheter des droits supplémentaires ou activer l'option de renouvellement automatique des abonnements.	6 avril 2022
Possibilité de suivre l'utilisation des licences	Les acheteurs peuvent désormais suivre les indicateurs de licence basés sur l'utilisation pour les produits AMI et SaaS avecAWS License Manager.	28 mars 2022
Mises à jour de la version Helm CLI	Mise à jour de la documentation des produits conteneurs concernant le changement de version de la CLI Helm de 3.7.0 à 3.7.1. Il s'agit de la seule version compatible pour le moment.	8 mars 2022

Mises à jour des politiques gérées existantes	Les autorisations qui n'étaient plus nécessaires ont été supprimées des politique s suivantes : `AWSMarket placeFullAccess` et`AWSMarketplaceImag eBuildFullAccess` .	4 mars 2022
Possibilité pour les acheteurs basés dans la région EMEA d'acheter des produits via Amazon Web Services EMEA SARL	AWS Marketplaceles acheteurs Comptes AWS basés dans des pays et territoires d'Europe, du Moyen-Orient et d'Afrique (EMEA), à l'exception de la Turquie et de l'Afrique du Sud, peuvent désormais recevoir des AWS Marketplace factures via Amazon Web Services EMEA SARL pour les achats effectués auprès de vendeurs éligibles à la zone EMEA.	7 janvier 2022
Support pour la région Asie-Pacifique (Jakarta)	AWS Marketplaceprend désormais en charge les Région AWS systèmes suivants : Asie-Pacifique (Jakarta).	13 décembre 2021
Méthode de livraison du tableau de bord pour les produits en conteneur	Les acheteurs peuvent désormais lancer des produits basés sur des conteneurs en installant un graphique Helm dans leurs environnements de lancement.	29 novembre 2021

Mises à jour générales et réorganisation de la documentation des produits basée sur les conteneurs	Documentation sur les produits basée sur des conteneurs mise à jour pour ajouter plus d'informations et de clarté sur la recherche, l'abonnement et le lancement de produits basés sur des conteneurs.	29 novembre 2021
Documentation ajoutée pour QuickLaunch	Les acheteurs peuvent désormais l'utiliser QuickLaunch lorsqu'ils lancent des produits basés sur des conteneurs avec une méthode de livraison Helm Chart. QuickLaunch est une fonctionnalité AWS Marketplace qui permet de AWS CloudFormation créer rapidement un nouveau cluster Amazon EKS et d'y lancer une application basée sur un conteneur.	29 novembre 2021
Tarification contractuelle pour les produits basés sur l'AMI et les produits basés sur des conteneurs	Les acheteurs peuvent désormais acheter un produit basé sur une AMI ou un produit basé sur un conteneur avec un prix initial.	17 novembre 2021
Support pour les bons de commande dans les produits SaaS	AWS Marketplaceprend en charge l'ajout de numéros de bon de commande aux contrats d'achat de logiciels en tant que service (SaaS).	28 octobre 2021

Support pour l'intégration de SAP Ariba	AWS Marketplaceprend en charge l'intégration avec le système d'approvisionnement SAP Ariba.	13 octobre 2021
Support pour les alias d'AMI	AWS Marketplaceprend en charge l'utilisation d'alias pour les ID d'AMI qui peuvent être utilisés dans toutes les régions.	8 septembre 2021
Suppression des autorisations non utilisées dans la politique gérée	Les autorisations non utilisées de la politique `AWSPrivateMarketplaceAdminFullAccess` AWS gérée ont été supprimées.	27 août 2021
Support pour le partage de licences via AWS License Manager	Vous pouvez partager les licences des produits que vous achetez avec d'autres comptes de votre AWS organisation.	3 décembre 2020
AWS Marketplacesoutient les offres de services professionnels	AWS Marketplaceprend désormais en charge l'achat de services professionnels.	3 décembre 2020
Support pour la devise préférée	Vous pouvez payer vos AWS Marketplace achats dans la devise de votre choix.	27 juillet 2020

Vous pouvez consulter et accepter les mises à niveau et les renouvellements des offres privées	Les vendeurs peuvent proposer des offres privées de mise à niveau et de renouvellement pour un contrat SaaS et un contrat SaaS avec des produits de consommation que vous pouvez consulter et accepter dans le cadre d'un contrat existant.	28 mai 2020
AWS Marketplaceprend en charge les produits de données via AWS Data Exchange	Vous pouvez désormais vous abonner aux produits de données AWS Data Exchange dansAWS Marketplace.	13 novembre 2019
AWS Marketplaceprend en charge les conteneurs payés à l'heure	AWS Marketplaceprend désormais en charge les conteneurs horaires payants exécutés sur Amazon Elastic Kubernetes Service (Amazon EKS).	25 septembre 2019
Offres privées mises à jour sur AWS Marketplace	Mise à jour du contenu pour plus d'informations sur l'acceptation de différents types d'offres privées.	29 mars 2019
Sécurité mise à jour sur AWS Marketplace	Informations sur les politiques IAM mises à jour, section restructurée pour plus de lisibilité.	25 mars 2019
Ajout de contenu pour la fonctionnalité de marché privé	Ajout de contenu prenant en charge le lancement de Private Marketplace.	27 novembre 2018

Première publication du guide de l'utilisateur pour les acheteurs	Première publication du guide de AWS Marketplace l'acheteur.	16 novembre 2018

AWS Glossaire

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

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.