



Guide de l'acheteur

# AWS Marketplace



# AWS Marketplace: Guide de l'acheteur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

---

# Table of Contents

Qu'est-ce que c'est AWS Marketplace ? .....	1
Structure du contrat dans AWS Marketplace .....	2
Mises à jour du CLUF .....	3
Contrats types pour AWS Marketplace .....	5
Utilisation en AWS Marketplace tant qu'acheteur .....	6
Logiciels et services sur AWS Marketplace .....	7
Différences entre AWS Marketplace et Amazon DevPay .....	9
Commencer en tant qu'acheteur .....	10
Achat de produits .....	10
Lancement des logiciels .....	11
Tutoriel : Acheter un produit logiciel basé sur l'AMI .....	12
Étape 1 : Création d'un Compte AWS .....	12
Étape 2 : Choix de votre logiciel .....	13
Étape 3 : Configuration de votre logiciel .....	14
Étape 4 : lancement de votre logiciel sur Amazon EC2 .....	15
Étape 5 : Gestion de votre logiciel .....	16
Étape 6 : mettre fin à votre instance .....	17
Pour plus d'informations .....	17
Régions prises en charge .....	18
Catégories de produits .....	20
Logiciels d'infrastructure .....	20
DevOps .....	21
Applications métier .....	22
Machine Learning (apprentissage automatique) .....	23
IoT .....	24
Services professionnels .....	25
Applications de bureau .....	25
Produits de données .....	27
Secteurs .....	27
Types de produit .....	28
Produits AMI .....	28
AWS CloudFormation modèle .....	29
Abonnements AMI .....	30
Produits AMI avec tarification contractuelle .....	33

Produits AMI activés pour le comptage .....	38
Étiquetage de répartition des coûts dans les produits AMI .....	39
Utilisation d'alias d'AMI .....	42
Produits de conteneur .....	44
Modèles de tarification pour les produits en conteneur payants .....	44
Présentation des conteneurs et de Kubernetes .....	45
Rechercher et s'abonner à des produits de conteneur .....	45
Produits en conteneur avec prix contractuel .....	50
Lancement d'un logiciel de conteneur .....	55
Produits de Machine Learning .....	61
Package SageMaker modèle Amazon .....	61
SageMaker Algorithme Amazon .....	62
Rechercher, s'abonner et déployer .....	63
Produits de services professionnels .....	66
Achat de services professionnels .....	66
Produits SaaS .....	67
Modèles de tarification .....	67
Lancement rapide .....	71
Produits de données .....	72
Payer pour des produits .....	73
Bons de commande .....	74
Utilisation des bons de commande pour les AWS Marketplace transactions .....	74
Utilisation de bons de commande pour l'utilisation de couvertures .....	76
Résolution des problèmes de bons de commande .....	76
Informations sur les remboursements .....	79
Annuler l'abonnement à votre produit .....	80
Résiliez votre abonnement SaaS .....	80
Annulation de votre abonnement au machine learning .....	80
Annulation de votre abonnement AMI .....	81
Annuler le renouvellement automatique de votre abonnement au contrat SaaS .....	82
Moyens de paiement .....	82
Erreurs de paiement .....	82
Devises supportées .....	83
Modifier votre devise préférée .....	84
Mise à jour des instructions de versement .....	85
Balisage de répartition des coûts .....	87

Étiquettes mesurées par le fournisseur .....	88
Rubriques en relation .....	42
Places de marché privées .....	90
Affichage des pages détaillées du produit .....	91
S'abonner à un produit sur une place de marché privée .....	91
Abonnement à un produit privé sur un marché privé .....	91
Demander l'ajout d'un produit à votre place de marché privée .....	92
Création et gestion d'une place de marché privée .....	92
Débuter avec le marché privé .....	92
Gestion du marché privé .....	93
Création d'une expérience de marché privée .....	95
Ajouter des produits à votre expérience de marché privé .....	95
Vérification des produits dans le cadre de votre expérience de marché privée .....	96
Personnalisation de votre expérience de marché privé .....	97
Gérer les audiences .....	97
Configuration de votre place de marché privée .....	97
Travailler avec des produits privés .....	98
Gestion des demandes des utilisateurs .....	99
Archivage et réactivation d'une expérience de marché privée .....	99
Offres privées .....	102
Types de produits éligibles aux offres privées .....	104
Préparation préalable à l'acceptation d'une offre privée .....	107
Vérification de vos préférences AWS Billing and Cost Management .....	107
Vérification de votre mode de paiement .....	107
Vérification de vos paramètres fiscaux .....	107
Affichage d'une offre privée et abonnement .....	108
Consulter et souscrire à une offre privée à partir d'une liste d'offres privées .....	108
Consulter et souscrire à une offre privée à partir d'un lien fourni par le vendeur .....	108
Consulter et souscrire à une offre privée depuis la page du produit .....	109
Résolution des problèmes liés aux offres privées .....	109
Je reçois un message d'erreur Page introuvable (404) lorsque je clique sur l'ID de l'offre pour afficher l'offre privée .....	110
Aucune de ces suggestions ne fonctionne .....	111
Page d'offres privées dans AWS Marketplace .....	111
Comprendre la page des offres privées .....	111
Autorisations requises pour consulter la page des offres privées .....	112

Abonnement à une offre privée SaaS .....	112
Abonnement à une offre privée AMI .....	116
Souscrire à une offre privée AMI annuelle avec un calendrier de paiement flexible .....	118
Souscrire à une offre privée AMI annuelle sans calendrier de paiement flexible .....	119
Modification de l'abonnement à une offre privée ou désabonnement .....	120
Passage de la tarification d'une offre publique à une offre privée .....	121
Modification d'un contrat SaaS : mises à niveau et renouvellements .....	121
Passage d'un abonnement SaaS à un contrat SaaS .....	122
Passage d'un contrat AMI à un nouveau contrat .....	122
Passage d'un abonnement AMI horaires à un abonnement AMI annuelles .....	122
Passage d'un abonnement AMI annuelles à un abonnement AMI horaires .....	123
Travailler avec de futurs accords datés .....	123
Création de futurs accords datés .....	124
Utilisation d'un planificateur de paiement flexible avec des accords futurs .....	124
Modification de vos futurs contrats .....	125
Réception de notifications concernant de futurs accords datés .....	125
Partage d'abonnements au sein d'une organisation .....	126
Conditions préalables au partage de licences .....	126
Afficher vos licences .....	127
Partage de vos licences .....	128
Suivi de l'utilisation des licences .....	128
Notifications .....	130
Notifications par e-mail .....	130
EventBridge Notifications Amazon .....	131
AWS Marketplace EventBridge Événements Amazon de l'API Discovery .....	131
Intégration du système d'approvisionnement .....	133
Comment fonctionne l'intégration des achats .....	133
Configuration de l'intégration du système d'approvisionnement .....	136
Configuration des autorisations IAM .....	136
Configuration AWS Marketplace en vue de l'intégration à Coupa .....	137
Configuration AWS Marketplace pour l'intégration à SAP Ariba .....	138
Codes UNSPSC utilisés par AWS Marketplace .....	140
Désactivation de l'intégration du système d'approvisionnement .....	141
Essais gratuits .....	142
Tarification des logiciels et de l'infrastructure .....	142
Essais gratuits pour les produits basés sur l'AMI .....	142

Essais gratuits pour les produits en conteneur .....	143
Essais gratuits pour les produits d'apprentissage automatique .....	143
Essais gratuits pour les produits SaaS .....	144
Utilisation du niveau gratuit d'AWS avec AWS Marketplace .....	145
Ajout d'abonnements AWS Marketplace à AWS Service Catalog .....	146
Commentaires sur les produits .....	147
Consignes .....	147
Restrictions .....	147
Délais et attentes .....	148
Obtention de support .....	150
AWS Marketplace Informations sur les fournisseurs .....	151
Commencer en tant qu'acheteur .....	152
Trouvez des produits grâce à AWS Marketplace Vendor Insights .....	152
Demandez l'accès aux données d'évaluation en vous abonnant .....	153
Se désabonner des données d'évaluation .....	154
Consulter le profil de sécurité d'un produit .....	154
Tableau de bord dans AWS Marketplace Vendor Insights .....	155
Afficher le profil de sécurité d'un produit SaaS .....	155
Comprendre les catégories de contrôle .....	156
Exportation d'instantanés .....	214
Exporter un instantané .....	152
.....	154
Contrôle de l'accès .....	215
Autorisations pour les acheteurs de AWS Marketplace Vendor Insights .....	216
GetProfileAccessTerms .....	216
ListEntitledSecurityProfiles .....	216
ListEntitledSecurityProfileSnapshots .....	216
GetEntitledSecurityProfileSnapshot .....	216
Sécurité activée AWS Marketplace .....	218
Informations sur l'abonné partagées avec les vendeurs .....	218
Mettre à niveau les politiques IAM vers IPv6 .....	219
Clients concernés par la mise à niveau d'IPv4 vers IPv6 .....	219
Qu'est-ce que l'IPv6 ? .....	219
Mise à jour d'une politique IAM pour IPv6 .....	220
Test du réseau après la mise à jour d'IPv4 vers IPv6 .....	221
Contrôle de l'accès aux abonnements à AWS Marketplace .....	223

Création de rôles IAM pour l'accès AWS Marketplace .....	223
AWS politiques gérées pour AWS Marketplace .....	224
Autorisations pour travailler avec License Manager .....	225
Ressources supplémentaires .....	225
AWS politiques gérées .....	225
AWSMarketplaceDeploymentServiceRolePolicy .....	227
AWSMarketplaceFullAccess .....	227
AWSMarketplaceLicenseManagementServiceRolePolicy .....	230
AWSMarketplaceManageSubscriptions .....	231
AWSMarketplaceProcurementSystemAdminFullAccess .....	232
AWSMarketplaceRead-uniquement .....	233
AWSPrivateMarketplaceAdminFullAccess .....	234
AWSPrivateMarketplaceRequests .....	236
AWS politique gérée : AWSServiceRoleForPrivateMarketplaceAdminPolicy .....	236
AWSVendorInsightsAssessorFullAccess .....	237
AWSVendorInsightsAssessorReadOnly .....	238
AWS Marketplace mises à jour des politiques AWS gérées .....	239
Trouver votre Compte AWS numéro pour le support client .....	242
Utilisation des rôles liés aux services .....	242
Rôles pour partager les droits .....	243
Rôles relatifs aux bons de commande .....	246
Rôles pour configurer et lancer AWS Marketplace des produits .....	249
Rôles pour configurer Private Marketplace .....	253
Création d'un administrateur de marché privé .....	257
Création de politiques personnalisées pour les administrateurs de marchés privés .....	258
Historique du document .....	262
AWS Glossaire .....	275
.....	cclxxvi



# Qu'est-ce que c'est AWS Marketplace ?

AWS Marketplace est 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 Marketplace comprend 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 et DevOps. AWS Marketplace simplifie également les licences et les achats de logiciels grâce à des options de tarification flexibles et à de multiples méthodes de déploiement. AWS Marketplace Inclut également les 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 par une seule source. AWS gère la facturation et les paiements, et les frais apparaissent sur votre AWS facture.

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

## Note

Les fournisseurs de produits de données doivent satisfaire aux critères d'éligibilité d'AWS Data Exchange. Pour plus d'informations, consultez la section [Fourniture de produits de données sur AWS Data Exchange](#) dans le guide de l'utilisateur d'AWS Data Exchange.

Chaque produit logiciel AWS Marketplace a fait l'objet d'un processus de curation. La page du produit peut contenir une ou plusieurs offres pour le produit. Lorsque le vendeur soumet un produit 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.

En AWS Marketplace, le produit peut être utilisé gratuitement ou peut être associé à des frais. Les frais font partie de votre AWS facture et, une fois que vous avez AWS Marketplace payé, vous payez 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 votre compte AWS. Le produit peut également être configuré pour utiliser AWS CloudFormation des modèles 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'un [contrat standard](#) avec une durée ou des limites d'utilisation spécifiées.

Une fois que les abonnements aux produits sont en place, vous pouvez les utiliser AWS Service Catalog pour copier le produit et gérer la manière dont il est accessible et utilisé dans votre organisation. Pour plus d'informations, consultez la section [Ajouter AWS Marketplace des produits à votre portefeuille](#) dans le guide de AWS Service Catalog l'administrateur.

## Structure du contrat dans AWS Marketplace

L'utilisation des logiciels, des services et des produits de données vendus AWS Marketplace est régie par des accords entre acheteurs et vendeurs. AWS n'est pas partie à ces accords.

En tant qu'acheteur, votre utilisation de AWS Marketplace est régie par les [conditions de service AWS](#), le [contrat client AWS](#) et la [déclaration de confidentialité](#).

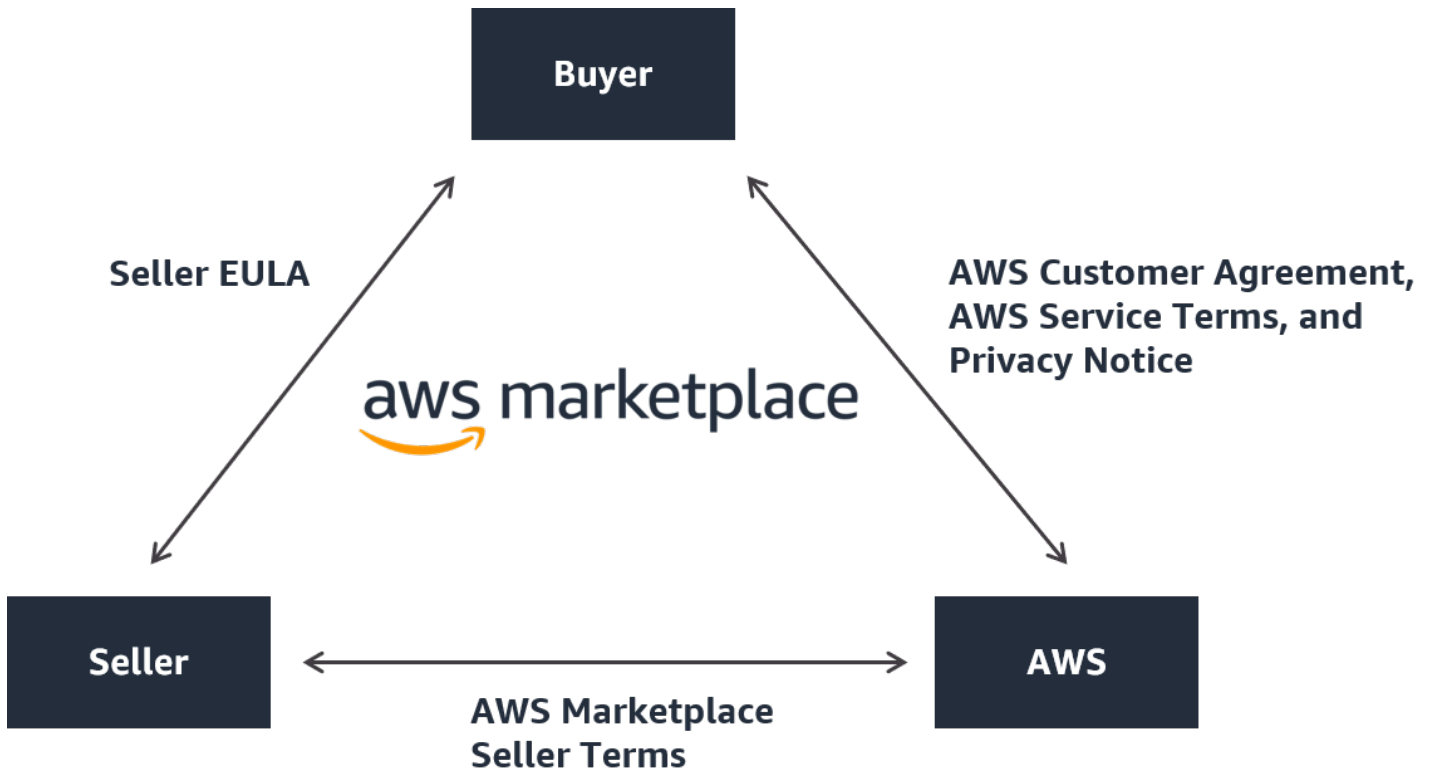
Les contrats de vente incluent les suivants :

- Le CLUF du vendeur se trouve sur la page de liste des produits pour les offres publiques de logiciels sur AWS Marketplace. De nombreux vendeurs utilisent le [contrat standard pour](#)

[AWS Marketplace \(SCMP\)](#) comme 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 Marketplace Les conditions](#) du vendeur régissent l'activité du vendeur dans AWS Marketplace.


Le graphique suivant montre la structure du contrat pour AWS Marketplace.



## Mises à jour du CLUF

Les vendeurs ont la possibilité de mettre à jour le CLUF pour chacun de leurs produits. La date d'entrée en vigueur de toute mise à jour dépendra de votre EULA, du type d'offre et du modèle de tarification.

Le tableau suivant fournit des informations sur la date d'entrée en vigueur d'un nouvel EULA.

 Note

Si vous et le vendeur avez conclu un accord personnalisé, les dispositions suivantes peuvent ne pas s'appliquer.

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 renouvellements de l'offre privée dépendent de l'offre privée spécifique.
Privé	Contrat	Votre offre privée actuelle expire et vous vous réinscrivez à l'offre publique ou à une nouvelle offre privée. Les renouvellements de l'offre

Type d'offre	Modèle de tarification	Lorsque le CLUF mis à jour entre en vigueur
		privée dépendent de l'offre privée spécifique.
Privé	Contrat avec consommation	Votre offre privée actuelle expire et vous vous réinscrivez à l'offre publique ou à une nouvelle offre privée. Les renouvellements de l'offre privée dépendent de l'offre privée spécifique.

## Contrats types pour AWS 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 offres, le [contrat standard pour AWS Marketplace \(SCMP\)](#). AWS Marketplace a 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. Les [termes du contrat](#) sont 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.
- [Addendum HIPAA Business Associate](#) — Soutient les transactions conformes aux exigences de conformité de la Health Insurance Portability and Accountability Act de 1996 (HIPAA).

Pour trouver des listes de produits proposant des contrats standardisés, utilisez le filtre Contrat standard lorsque vous recherchez des 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, voir [Contrats standardisés dans AWS Marketplace](#).

## Utilisation en AWS Marketplace tant qu'acheteur

En tant qu'acheteur, vous pouvez [AWS Marketplace](#) 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 vous connectez à votre page d'abonnement Compte AWS et vous êtes redirigé vers une page d'abonnement contenant le CLUF, les conditions générales d'utilisation et toutes les options disponibles pour personnaliser votre abonnement.

AWS Marketplace les 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 leurs achats AWS Marketplace. Pour plus d'informations sur les taxes, consultez la [page d'aide fiscale d'AWS Marketplace Buyers Tax](#).

Pour plus d'informations sur Amazon Web Services EMEA SARL, consultez les FAQ [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 de passer par AWS Inc. Pour plus d'informations, consultez la section [Paiement des produits](#).

Une fois l'abonnement traité, vous pouvez configurer les options d'expédition, les versions du logiciel et l' Région AWS endroit où vous souhaitez utiliser le produit, puis lancer le produit logiciel. Vous pouvez également trouver ou lancer vos produits en vous rendant sur [Your Marketplace Software](#) sur le AWS Marketplace site Web, depuis votre console AWS Marketplace ou celle d'Amazon Elastic Compute Cloud (Amazon EC2), ou via le Service Catalog.

Pour plus d'informations sur les catégories de produits disponibles à AWS Marketplace l'aide de [Catégories de produits](#).

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

- [Produits AMI](#)
- [Produits de conteneur](#)
- [Produits de Machine Learning](#)
- [Produits de services professionnels](#)
- [Produits SaaS](#)
- Produits de données — Voir [Qu'est-ce qu'AWS Data Exchange ?](#) dans le guide de l'utilisateur d'AWS Data Exchange

## Logiciels et services sur AWS Marketplace

AWS Marketplace propose de nombreuses catégories de logiciels, notamment des bases de données, des serveurs d'applications, des outils de test, des outils de surveillance, de gestion de contenu et de 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 l'utiliser AWS CloudFormation pour déployer une topologie du produit.

N'importe quel AWS client peut faire ses achats sur AWS 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, en utilisant les instruments de paiement déjà enregistrés auprès de AWS. Les frais du logiciel apparaissent sur la même facture mensuelle que les frais d'infrastructure AWS .

### Remarques

- De nombreux produits professionnels sont disponibles dans le AWS Marketplace, notamment des logiciels en tant que service (SaaS) 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 didacticiels présentés dans [Tutorial : Get Started with Amazon EC2 Linux instances](#) peuvent vous aider à apprendre les bases d'Amazon EC2.

- Si vous envisagez de lancer des topologies complexes de AWS Marketplace produits par le biais d'AWS CloudFormation, [Getting Started with AWS CloudFormation](#) peut vous aider à acquérir des connaissances de CloudFormation base utiles sur AWS.

AWS Marketplace inclut les catégories de logiciels suivantes :

- 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 grande catégorie de logiciels contient des sous-catégories plus spécifiques. Par exemple, la catégorie Logiciels d'infrastructure contient des sous-catégories telles que le développement d'applications, les bases de données et la mise en cache, et les systèmes d'exploitation. Les logiciels sont disponibles sous la forme de sept types de produits différents, dont Amazon Machine Images (AMI) et le logiciel en tant que service (SaaS). Pour plus d'informations sur les différents types de logiciels, consultez [Types de produit](#).

Pour vous aider à choisir le logiciel dont vous avez besoin, AWS Marketplace fournit 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 AWS Marketplace et Amazon DevPay

Il existe des différences substantielles entre AWS Marketplace et Amazon DevPay. Les deux aident les clients à acheter des logiciels qui fonctionnent sur Amazon AWS, mais qui AWS Marketplace offrent une expérience plus complète DevPay. Pour les acheteurs de logiciels, les différences clés sont les suivantes :

- AWS Marketplace propose une expérience d'achat similaire à celle d'Amazon.com, en simplifiant la découverte des logiciels disponibles.
- AWS Marketplace les produits fonctionnent avec d'autres AWS fonctionnalités telles que le cloud privé virtuel (VPC) et peuvent être exécutés sur des instances réservées et des instances ponctuelles Amazon Elastic Compute Cloud (Amazon EC2), en plus des instances à la demande.
- AWS Marketplace prend en charge les logiciels soutenus par Amazon Elastic Block Store (Amazon EBS), ce qui n'est pas le cas d'Amazon DevPay .

De plus, les vendeurs de logiciels bénéficient de la portée marketing et de la facilité de découverte de AWS Marketplace.

# Commencer en tant qu'acheteur

Les rubriques suivantes décrivent le processus de démarrage des produits logiciels en tant qu'AWS Marketplace acheteur.

## Rubriques

- [Achat de produits](#)
- [Lancement des logiciels](#)
- [Tutoriel : Acheter un produit logiciel basé sur l'AMI](#)
- [Pour plus d'informations](#)

Pour plus d'informations sur la prise en main des produits de données, consultez la section [Abonnement aux produits de données sur AWS Data Exchange](#) dans le guide de l'utilisateur d'AWS Data Exchange.

## Achat de produits

En AWS Marketplace, l'achat d'un produit signifie que vous avez accepté les conditions du produit telles qu'indiquées sur la page détaillée 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 votre adresse Compte AWS pour les offres acceptées dans AWS Marketplace.

### Note

AWS offre la possibilité de demander des démonstrations guidées pour certains produits gratuitement. AWS Marketplace Si une démonstration guidée est disponible, un bouton Demander une démonstration s'affichera sur la page détaillée du produit. Pour demander une démonstration, cliquez sur le bouton et fournissez les détails de la demande. Vous recevrez un e-mail de confirmation résumant votre demande, et un AWS représentant vous contactera.

Si le produit est soumis à des frais mensuels ou s'il est acheté dans le cadre d'un contrat d'abonnement, les frais vous sont facturés lors de l'abonnement. L'abonnement est calculé au prorata du temps restant dans le mois. Aucun autre frais n'est facturé tant que vous n'avez pas pris l'une des mesures suivantes :

- Lancez une instance Amazon Elastic Compute Cloud (Amazon EC2) avec le produit Amazon Machine Image (AMI).
- Déployez le produit à l'aide d'un AWS CloudFormation modèle.
- 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, consultez la section [Abonnement aux produits de données sur AWS Data Exchange](#) dans le guide de l'utilisateur d'AWS Data Exchange.

## 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 outils de gestion Amazon Web Services (AWS), notamment la console Amazon Elastic Compute Cloud (Amazon EC2) AWS Management Console, les API Amazon EC2 ou la console. AWS CloudFormation

Grâce à la vue de lancement en un clic, vous pouvez rapidement consulter, modifier puis lancer une instance unique du logiciel avec les paramètres recommandés par le vendeur du logiciel. La vue Lancer avec la console EC2 permet de trouver facilement le numéro d'identification de l'AMI et les autres informations pertinentes requises pour lancer l'AMI à l' AWS Management Console aide des API Amazon EC2 ou d'autres outils de gestion. La vue Lancer avec la console EC2 fournit également davantage d'options de configuration que le lancement depuis le AWS Management Console, comme le balisage d'une instance.

### Note

Si vous ne parvenez pas à accéder à un type d'instance ou Région AWS s'il n'était peut-être pas pris en charge au moment où l'offre privée vous a été envoyée. Consultez les détails de votre contrat pour plus d'informations. Pour accéder à une instance ou à une

région, contactez le vendeur et demandez une offre privée actualisée. Après avoir accepté la nouvelle offre, vous aurez accès à l'instance ou à la région que vous venez d'ajouter.

Pour les AWS Marketplace produits dotés de topologies complexes, la vue de lancement personnalisé propose une option de lancement avec CloudFormation console qui charge le produit dans la AWS CloudFormation console avec le AWS CloudFormation modèle approprié. Vous pouvez ensuite suivre les étapes de l'assistant de AWS CloudFormation console pour créer le cluster d'AMI et les AWS ressources associées pour ce produit.

## Tutoriel : Acheter un produit logiciel basé sur l'AMI

Le didacticiel suivant explique comment acheter un produit Amazon Machine Image (AMI) avec AWS Marketplace.

### Étapes

- [Étape 1 : Création d'un Compte AWS](#)
- [Étape 2 : Choix de votre logiciel](#)
- [Étape 3 : Configuration de votre logiciel](#)
- [Étape 4 : lancement de votre logiciel sur Amazon EC2](#)
- [Étape 5 : Gestion de votre logiciel](#)
- [Étape 6 : mettre fin à votre instance](#)

### Étape 1 : Création d'un Compte AWS

Vous pouvez naviguer sur le AWS Marketplace site Web (<https://aws.amazon.com/marketplace>) sans être connecté à votre Compte AWS. Cependant, vous devez vous connecter pour vous abonner ou lancer des produits.

Vous devez être connecté à votre compte Compte AWS pour accéder à la AWS Marketplace console. Pour plus d'informations sur la création d'un Compte AWS, reportez-vous à la section [Création d'un Compte AWS](#) dans le Guide de AWS Account Management référence.

## Étape 2 : Choix de votre logiciel

### Choisir vos logiciels

1. Accédez au [AWS Marketplace site Web](#).

#### Note

Vous pouvez acheter, vous abonner et lancer de nouvelles instances depuis le AWS Marketplace site Web public, à l'[adresse https://aws.amazon.com/marketplace](https://aws.amazon.com/marketplace), ou via AWS Marketplace le AWS Management Console site <https://console.aws.amazon.com/marketplace/home#/subscriptions>.

Les expériences sur les deux sites sont similaires. Cette procédure utilise le AWS Marketplace site Web mais note les différences majeures 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 Acheter toutes les catégories, sélectionnez Gestion de contenu.
3. Dans la liste de gestion de contenu, choisissez WordPressCertified by 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 les types d'instances de chaque type Région 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 encore connecté, vous êtes invité à vous connecter à AWS Marketplace. Si vous en avez déjà un Compte AWS, vous pouvez utiliser ce compte pour vous connecter. Si vous n'en avez pas déjà un Compte AWS, consultez [Étape 1 : Création d'un Compte AWS](#).
7. Lisez les conditions de l'offre Bitnami, puis choisissez Accepter le contrat pour accepter l'offre d'abonnement.

8. La fin de l'opération d'abonnement peut prendre un certain temps. Lorsque c'est le cas, vous recevez un e-mail concernant les conditions d'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 seront facturés lors de l'abonnement, qui sont calculés au prorata du temps restant dans le mois. Aucun autre frais ne sera facturé tant que vous n'aurez pas lancé une instance Amazon Elastic Compute Cloud (Amazon EC2) avec l'AMI que vous avez choisie.

#### Note

En tant qu'abonné à un produit, votre compte recevra 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 livraison, la version et Région AWS l'utilisation que vous souhaitez utiliser.

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 AMI est de la forme `ami-<identifiant>`, par exemple `ami-123example456`. Chaque version de chaque produit dans chaque région possède une AMI différente. Cet ID d'AMI vous permet de spécifier l'AMI correcte à utiliser lors du lancement du produit. L'Ami Alias est un identifiant similaire qui est plus facile à utiliser en automatisation.

Pour plus d'informations sur l'alias AMI, consultez [Utilisation d'alias d'AMI](#).

4. Sélectionnez Continuer jusqu'au lancement.

## Étape 4 : lancement de votre logiciel sur Amazon EC2

Avant de lancer votre instance Amazon EC2, vous devez décider si vous souhaitez le lancer avec un lancement en un clic ou si vous souhaitez le lancer à l'aide de la console Amazon EC2. Le lancement en 1 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 voir votre facture mensuelle estimée. Si vous préférez d'autres options, telles que le lancement dans un Amazon Virtual Private Cloud (Amazon VPC) ou l'utilisation d'instances Spot, vous devez le lancer à l'aide de 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 le menu déroulant Choisir une action, puis vérifiez les paramètres par défaut. Pour modifier l'un d'eux, effectuez l'une des opérations suivantes :
  - Dans la liste déroulante Type d'instance EC2, choisissez un type d'instance.
  - Dans les listes déroulantes Paramètres VPC et Paramètres de 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 plus d'informations sur les groupes de sécurité, consultez les groupes de [sécurité Amazon EC2 pour les instances Linux](#) dans le guide de l'utilisateur Amazon EC2.
  - Déployez Key Pair (Paire de clés), puis choisissez une paire de clés existante, si vous en avez une. Si vous n'avez pas de paire de clés, vous êtes invité à en créer une. Pour plus d'informations sur les paires de clés Amazon EC2, consultez la section paires de clés [Amazon EC2](#).
2. Lorsque vous êtes satisfait de vos paramètres, choisissez Launch.

Votre nouvelle instance est lancée avec les logiciels WordPress Certified by Bitnami et Automattic exécutés dessus. À partir de là, vous pouvez consulter les détails de l'instance, en créer une autre ou afficher toutes les instances de votre logiciel.

## Lancement sur Amazon EC2 à l'aide de Launch avec la console EC2

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 de l'AMI dans la liste Sélectionnez 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 de la [section Commencer 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 en AWS Marketplace utilisant la page Gérer les abonnements de la [AWS Marketplace console](#).

Pour gérer vos logiciels

1. Accédez à la [AWS Marketplace console](#), puis 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 : mettre fin à 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 interrompue. Toutefois, vous pouvez lancer des instances supplémentaires de la même AMI.

Pour mettre fin à une instance

1. Accédez à la [AWS Marketplace console](#), puis 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 à laquelle vous souhaitez mettre fin. Cela ouvre la console Amazon EC2 et affiche les instances de cette région dans un nouvel onglet. Si nécessaire, vous pouvez revenir sur cet onglet pour voir l'ID d'instance de l'instance à fermer.
5. Dans la console Amazon EC2, choisissez l'ID de l'instance pour ouvrir la page des détails de l'instance.
6. Dans la liste déroulante État de l'instance, sélectionnez **Terminate instance**.
7. Choisissez **Résilier** lorsque vous êtes invité à confirmer.

La résiliation prend 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 plus AWS, consultez <https://aws.amazon.com/>.

# Pris en charge Régions AWS 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 AWS Marketplace site Web 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

Le [AWS Marketplace](#) site Web est organisé en catégories principales, avec des sous-catégories sous chacune d'elles. Vous pouvez effectuer des recherches et filtrer en fonction des catégories et des sous-catégories.

## Rubriques

- [Logiciels d'infrastructure](#)
- [DevOps](#)
- [Applications métier](#)
- [Machine Learning \(apprentissage automatique\)](#)
- [IoT](#)
- [Services professionnels](#)
- [Applications de bureau](#)
- [Produits de données](#)
- [Secteurs](#)

## Logiciels d'infrastructure

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

### Backup et restauration

Produits utilisés pour des solutions de stockage et de sauvegarde.

### Analyses de données

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

Les applications étaient axées sur les rôles liés au stockage.

# DevOps

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

## Gestion agile du cycle de vie

Produits utilisés pour Agile SDLM.

## 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 continue et livraison continue

Produits utilisés pour le CI/CD.

## L'infrastructure en tant que code

Produits utilisés pour les infrastructures.

## Suivi des problèmes et 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 et productivité

Produits utilisés pour faciliter la collaboration dans votre entreprise.

## Centre de contact

Produits utilisés pour activer les 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 fournissant des solutions de commerce électronique.

## Formation en ligne

Des produits qui fournissent des solutions d'apprentissage en ligne.

## Ressources humaines

Produits utilisés pour renforcer les ressources humaines au sein de votre organisation.

## Gestion d'entreprise informatique

Produits utilisés pour permettre la gestion des activités informatiques dans 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 proposent des algorithmes d'apprentissage automatique et des packages de modèles compatibles 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 classification, le regroupement, l'édition/le traitement, l'intégration, la génération, la grammaire/

l'analyse syntaxique, l'identification, la reconnaissance des noms et des entités, l'analyse des sentiments, la synthèse et la traduction. text-to-speech

## 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 classification, la détection d'objets, l'édition/le traitement, la détection des anomalies, l'identification du locuteur, le mouvement, la réidentification, le résumé, le texte/sous-titrage et le suivi.

## Audio

Produits qui fournissent la capacité d'analyse audio. Les exemples incluent l'identification des speech-to-text locuteurs, la classification, l'identification des 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 intelligentes

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 aux AWS Marketplace produits.

### 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 l'installation et au déploiement de logiciels tiers.

### Managed Services

Gestion de end-to-end l'environnement électronique en votre nom.

### Premium Support

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

### Entraînement

Des ateliers, des programmes et des outils pédagogiques 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 Data Exchange](#).

## Secteurs

### Éducation et recherche

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 et sciences de la vie

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

### Médias et divertissement

Produits et solutions liés au contenu multimédia.

### Industriel

Produits et solutions liés à l'industrie.

### Énergie

Produits et solutions liés à l'énergie.

# Types de produit

AWS Marketplace inclut 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 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 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 dessus AWS.

Le logiciel répertorié dans AWS Marketplace est uniquement disponible pour être exécuté sur Amazon Elastic Compute Cloud (Amazon EC2). Il n'est pas disponible au téléchargement.

Vous pouvez également 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. AWS Marketplace La qualité de tous les AWS Marketplace produits a été vérifiée et préconfigurés pour être lancés en un clic sur l'infrastructure Amazon Web Services (AWS).

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 ceux d'un client Compte 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.

Le AWS Marketplace catalogue contient une sélection de logiciels open source et commerciaux de vendeurs renommés. De nombreux produits AWS Marketplace peuvent 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.

Un AWS Marketplace produit contient une AMI pour chaque produit Région AWS dans lequel il 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.

Certains AWS Marketplace produits peuvent lancer plusieurs instances d'une AMI car ils sont déployés en tant que cluster à l'aide AWS CloudFormation de modèles. Ce cluster d'instances, ainsi que les services AWS d'infrastructure supplémentaires configurés par le CloudFormation modèle, constituent un déploiement de produit unique.

## AWS CloudFormation modèle

### Important

AWS Marketplace supprimera le mode de livraison pour plusieurs produits Amazon Machine Image (AMI) utilisant des AWS CloudFormation modèles en août 2024. AWS Marketplace Les autres produits CloudFormation utilisés, tels que l'AMI unique avec CloudFormation, ne seront pas affectés.

Jusqu'en août 2024, les abonnés existants peuvent lancer de nouvelles instances de leurs multiples produits AMI à l'aide de CloudFormation modèles provenant de AWS 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 à fonctionner.

Si vous avez des questions, contactez [AWS Support](#).

AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à les gérer et plus de temps à vous concentrer sur les applications qui s'exécutent AWS. Un CloudFormation modèle décrit les différentes AWS ressources dont vous avez besoin, telles que les instances Amazon Elastic Compute Cloud (Amazon

EC2) ou les instances de base de données Amazon Relational Database Service (Amazon RDS). CloudFormation s'occupe du provisionnement et de la configuration de ces ressources pour vous. Pour plus d'informations, consultez [Getting started with AWS CloudFormation](#).

## Utilisation de AWS CloudFormation modèles

Les vendeurs de logiciels peuvent proposer CloudFormation des modèles pour définir une topologie de déploiement préférée composée de plusieurs instances d'AMI et d'autres AWS ressources. Si un CloudFormation modèle est disponible pour un produit, il sera répertorié comme 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 un CloudFormation modèle pour déployer plusieurs instances d'une AMI agissant en tant que cluster, ainsi que des AWS ressources telles qu'Amazon RDS, Amazon Simple Storage Service (Amazon S3) ou tout autre service, en tant que solution unique. AWS

### Rubriques

- [Abonnements AMI dans AWS Marketplace](#)
- [Produits AMI avec tarification contractuelle](#)
- [Produits AMI activés pour le comptage](#)
- [Étiquetage de répartition des coûts dans les produits AMI](#)
- [Utilisation d'alias d'AMI](#)

## Abonnements AMI dans AWS Marketplace

En AWS Marketplace, 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 pendant les 12 prochains mois. Vous pouvez souscrire un abonnement annuel à un produit AWS Marketplace logiciel sur une instance Amazon Elastic Compute Cloud (Amazon EC2).

### Note

Pour les AMI à tarif horaire annuel, l'abonnement annuel ne couvre que les types d'instances que vous spécifiez lors de l'achat. Par exemple, `t3.medium`. Le lancement de tout autre type d'instance entraîne le tarif horaire correspondant à ce type d'instance en fonction de l'abonnement actif.

Vous pouvez également continuer à lancer et à exécuter des produits AWS Marketplace logiciels en utilisant la tarification horaire. Les frais d'utilisation d'Amazon EC2 et des autres services fournis par Amazon EC2 AWS sont distincts et s'ajoutent à ceux que vous payez pour acheter des produits AWS 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. Cependant, le formulaire de licence AMI AWS Marketplace passera automatiquement à la tarification horaire.

Si un produit horaire AMI n'est pas compatible avec 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 se rendre sur la page du produit AWS Marketplace et acheter des contrats annuels. Chaque contrat annuel permet à l'acheteur d'exécuter une instance sans avoir à payer le taux horaire. Les contrats varient en fonction du type d'instance.

## Modifications de l'accord annuel

Avec les modifications horaires annuelles (annuelles) du plan, vous pouvez modifier votre plan directement depuis le Portail de gestion AWS Marketplace. Vous pouvez utiliser des modifications lorsque vous devez changer l'AMI pour qu'elle s'exécute sur un type d'instance Amazon Elastic Compute Cloud (Amazon EC2) doté d'un plus grand nombre de vCPU, ou passer à une génération plus moderne d'architecture de processeur. Grâce aux modifications, vous pouvez apporter les modifications suivantes à votre plan annuel existant :

- Basculer entre les familles de types d'instances Amazon EC2
- Basculer entre les tailles de type d'instance Amazon EC2
- Ajouter un nouveau type d'instance
- Augmenter la quantité d'un type d'instance existant dans le contrat

Tous les nouveaux types d'instances Amazon EC2 que vous ajoutez ou vers lesquels vous passez dans le contrat seront désignés conjointement avec la date de fin actuelle du plan, de sorte que tous les types d'instances du contrat seront renouvelés en même temps.

Vous pouvez apporter une modification tant que le coût proportionnel de la modification est supérieur à zéro. Le coût au prorata des instances Amazon EC2 récemment ajoutées est basé sur le coût annuel du type d'instance ajusté pour la durée restante du contrat. Lorsque vous changez de type d'instance, le coût au prorata du type d'instance Amazon EC2 supprimé est déduit du coût au prorata du type d'instance Amazon EC2 récemment ajouté.

**Note**

Les modifications sont prises en charge pour tous les accords conclus à partir d'offres publiques et pour les accords issus d'offres privées sans plans de versement.

## Exemples de modifications d'accords annuels

Examinez les exemples suivants relatifs aux modifications des accords annuels. Dans les exemples suivants, le client a signé un contrat le 1er janvier 2024 pour deux unités de types d'instances m5.large (4 000\$ par an). Le vendeur reçoit 8 000\$, moins les frais de mise en vente.

### Exemple 1 : Passage à un type d'instance de valeur égale

En milieu d'année, le client souhaite passer d'une unité du type d'instance m5.large à une unité du type d'instance r5.large. Le coût proportionnel du changement est calculé en déduisant le coût proportionnel de l'instance supprimée (six mois de m5.large - 2 000\$) du coût proportionnel de l'instance ajoutée (six mois de r5.large - 2 000\$). Le coût net étant de 0\$, la modification peut avoir lieu.

### Exemple 2 : Passage à un type d'instance plus onéreux

En milieu d'année, le client souhaite passer d'une unité du type d'instance m5.large à une unité du type d'instance m5.2xlarge. Le coût proportionnel du changement est calculé en déduisant le coût proportionnel de l'instance supprimée (six mois de m5.large - 2 000\$) du coût proportionnel de l'instance ajoutée (six mois de m5.2xlarge - 3 000\$). Le coût net étant de 1 000\$, la modification peut être apportée.

### Exemple 3 : Passage à une seule unité d'un type d'instance moins cher

En milieu d'année, le client souhaite passer d'une unité du type d'instance m5.large à une unité du type d'instance c5.large. Le coût proportionnel du changement est calculé en déduisant le coût proportionnel de l'instance supprimée (6 mois de m5.large - 2 000\$) du coût proportionnel de l'instance ajoutée (6 mois de c5.large - 1 500\$). Le coût net étant de -500 \$ (moins de 0\$), la modification ne peut pas avoir lieu.



#### Exemple 4 : Passage à plusieurs unités d'un type d'instance moins cher

En milieu d'année, le client souhaite passer d'une unité du type d'instance m5.large à deux unités du type d'instance c5.large. Le coût proportionnel du changement est calculé en déduisant le coût proportionnel de l'instance supprimée (six mois de m5.large - 2 000\$) du coût proportionnel des instances ajoutées (six mois de deux instances c5.large - 3 000\$). Le coût net étant de 1 000\$, la modification peut être apportée.

#### Exemple 5 : Ajouter un nouveau type d'instance

En milieu d'année, le client souhaite ajouter une unité supplémentaire du type d'instance m5.large au contrat. Le coût proportionnel de cette modification est calculé comme le coût proportionnel de l'instance ajoutée (six mois de m5.large - 2 000\$). Le coût net étant de 2 000\$, la modification peut être apportée.

#### Exemple 6 : Supprimer un type d'instance

En milieu d'année, le client souhaite supprimer une unité du type d'instance m5.large. Le coût proportionnel de cette modification est calculé comme le coût proportionnel de l'instance supprimée (six mois de m5.large - 2 000\$). Le coût net étant de -2 000\$ (moins de 0\$), la modification ne peut pas avoir lieu.

## Produits AMI avec tarification contractuelle

Certains vendeurs proposent des produits logiciels publics basés sur Amazon Machine Image (AMI) avec un modèle de tarification contractuelle. Dans ce modèle, vous acceptez d'effectuer un paiement initial unique pour des quantités distinctes de licences afin d'accéder au produit logiciel pendant une durée de votre choix. Vous êtes facturé, à l'avance, par le biais de votre Compte AWS. 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 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 en consultant 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 AMI avec offre publique de prix contractuels

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

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 voir les unités et le taux pour chaque durée (en mois).

3. Choisissez Continuer à vous abonner pour démarrer l'abonnement.

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. Une fois que vous avez effectué vos sélections, cliquez sur Create Contract (Créer contrat).

Le prix total du contrat vous est facturé Compte AWS. Une licence est générée dans AWS License Manager.

### Note

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

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

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

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. 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 sur votre AWS License Manager compte pour le produit logiciel peuvent prendre jusqu'à 10 minutes.

## Accès au logiciel

Pour accéder au produit logiciel basé sur l'AMI

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, passez en revue votre configuration et choisissez la manière dont vous souhaitez lancer le logiciel sous Choisir une action.
  4. Dans le champ Choisissez un type d'instance, choisissez une instance Amazon Elastic Compute Cloud (Amazon EC2), puis choisissez Next : Configure Instance Details.
  5. Sur la page Configurer les détails de l'instance, pour le rôle IAM, choisissez un rôle AWS Identity and Access Management (IAM) existant dans votre. Compte AWS

Si vous n'avez pas de rôle IAM, cliquez sur le lien Créer un nouveau rôle IAM manuellement et suivez les instructions.

#### Note

Lorsque vous achetez un produit dont le prix est contractuel, une licence est créée par celui-ci AWS Marketplace , Compte AWS que 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 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": "*"
    }
  ]
}
```

}

6. Une fois les détails de l'instance configurés, choisissez Review and Launch.
7. Sur la page Review Instance Launch, sélectionnez une paire de clés existante ou créez-en une nouvelle, puis choisissez Launch Instances.

La fenêtre de progression du lancement de l'instance initiale apparaît.

8. Une fois l'instance initiée, accédez au tableau de bord EC2 et, sous Instances, vérifiez que l'état de l'instance indique En cours d'exécution.

## Afficher une licence générée

Pour consulter une licence générée

1. Connectez-vous à l' AWS License Manager aide de votre Compte 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 AMI, AWS Marketplace les acheteurs peuvent modifier certains aspects du contrat. Un contrat AMI 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 à AWS 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 le renouvellement automatique.

## Produits AMI activés pour le comptage

Certains produits listés sur le AWS Marketplace site 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. Un rôle IAM autorisé à mesurer l'utilisation doit être associé à votre instance AWS Marketplace Amazon Elastic

Compute Cloud (Amazon EC2) au moment du lancement. Pour plus d'informations sur les rôles IAM pour Amazon EC2, [consultez Rôles IAM pour Amazon EC2](#).

## Étiquetage de répartition des coûts dans les produits AMI

AWS Marketplace prend en charge le balisage 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'AMI correspondante. AWS Marketplace Vous pouvez utiliser les balises de répartition des coûts activées pour identifier et suivre l'utilisation des AMI via AWS Cost Explorer les rapports sur les AWS coûts et l'utilisation, AWS les budgets ou d'autres outils d'analyse des dépenses dans le cloud.

Le fournisseur qui a fourni l'AMI peut également enregistrer d'autres étiquettes personnalisées dans le comptage des 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. Après avoir activé les balises de répartition des coûts, AWS utilise les balises de répartition des coûts pour organiser les coûts des ressources dans votre rapport de répartition des coûts, afin de faciliter la catégorisation et le suivi de vos AWS coûts.

Le balisage de répartition des coûts permet de suivre les coûts uniquement à partir du moment où les balises ont été activées dans la console Billing and Cost Management. Seuls Compte AWS les propriétaires, les titulaires de comptes de AWS Organizations gestion et les utilisateurs disposant des autorisations appropriées peuvent accéder à la console Billing and Cost Management pour un compte. Que vous utilisiez ou non le balisage de répartition des coûts, le montant qui vous est facturé ne change pas. L'utilisation de balises de répartition des coûts n'a aucun impact sur les fonctionnalités de vos produits logiciels basés sur l'AMI.

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

Chaque instance Amazon EC2 lancée pour un abonnement AWS Marketplace AMI est associée à une rubrique d'utilisation AWS Marketplace logicielle correspondante dans le rapport AWS Cost and Usage. Votre AWS Marketplace utilisation reflétera toujours les balises spécifiques appliquées à l'instance Amazon EC2 correspondante. Cela vous permet de distinguer vos coûts AWS Marketplace d'utilisation en fonction des différentes valeurs de balise attribuées, au niveau de l'instance.

Vous pouvez également additionner vos coûts d'utilisation basés sur les balises pour égaler les frais d'utilisation du logiciel AMI indiqués sur votre facture à l'aide du rapport Cost Explorer ou du rapport AWS Cost and Usage.

## Recherche de budgets avec des instances balisées allouées aux coûts

Si vous avez déjà filtré des budgets actifs sur des balises de répartition des coûts sur un certain nombre d'instances Amazon EC2 dans la console Billing and Cost Management, il peut être difficile de tous les trouver. Le script Python suivant renvoie une liste de budgets contenant des instances Amazon EC2 à partir de votre budget AWS Marketplace actuel. Région 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 de AWS Billing l'utilisateur.
- [Activation des balises de répartition des coûts générées par AWS](#) dans le guide de l'AWS Billing utilisateur.
- [Marquage de vos ressources Amazon EC2](#) dans le guide de l'utilisateur Amazon EC2.

## Utilisation d'alias d'AMI

Une Amazon Machine Image (AMI) est identifiée par un AMI ID. Vous pouvez utiliser le AMI ID pour indiquer l'AMI que vous souhaitez utiliser lors du lancement d'un produit. AMI IDII a la forme `ami-identifiant`, par exemple, `ami-123example456`. Chaque version de chaque produit Région AWS possède une AMI différente (et différente AMI ID).

Lorsque vous lancez un produit à partir de AWS Marketplace, AMI ID il est automatiquement renseigné pour vous. AMI IDII est utile d'en disposer si vous souhaitez automatiser le lancement de produits depuis AWS Command Line Interface (AWS CLI) ou en utilisant Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez trouver le AMI ID moment où vous configurez votre logiciel au moment du lancement. Pour plus d'informations, consultez [Étape 3 : Configuration de votre logiciel](#).

Ami AliasII se trouve également au même endroit que le AMI ID, lors de la configuration de votre logiciel. Ami AliasII s'agit d'un identifiant similaire au AMI ID, mais il est plus facile à utiliser en automatisation. An AMI alias a la forme `aws/service/marketplace/prod-identifiant/version`, par exemple, `aws/service/marketplace/prod-1234example5678/12.2`. Vous pouvez utiliser cet Ami Alias identifiant dans n'importe quelle région et le mapper AWS automatiquement à la région appropriée 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 le « AMI alias so » qui AWS choisit pour vous la version la plus récente du produit, par exemple, `aws/service/marketplace/prod-1234example5678/latest`.

**⚠ Warning**

L'utilisation de **latest** cette option vous permet d'accéder à la version la plus récente du logiciel. Toutefois, utilisez cette fonctionnalité avec prudence. Par exemple, si les versions 1.x et 2.x d'un produit sont disponibles, vous utilisez peut-être la version 2.x. Cependant, la version la plus récente du produit peut corriger un bogue pour la version 1.x.

## Exemples d'utilisation des alias d'AMI

Les alias d'AMI sont utiles dans le cadre de l'automatisation. Vous pouvez les utiliser dans AWS CLI ou dans les AWS CloudFormation modèles.

L'exemple suivant montre comment utiliser un alias d'AMI pour lancer une instance à l'aide du AWS CLI.

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

L'exemple suivant montre un CloudFormation modèle qui accepte l'alias AMI comme 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 ainsi que de plus amples informations sur chacun d'entre eux, consultez [Services 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, consultez [QuickLaunch dans AWS Marketplace](#).

Cette section fournit des informations sur la recherche, l'abonnement et le lancement de produits conteneurisés dans AWS 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 payants AWS 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 AWS d'orchestration hautement évolutif et performant, et Amazon EKS, qui facilite le déploiement, la gestion et le dimensionnement des [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, consultez [Modes 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, consultez [Services 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 Marketplace site 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 produit AWS 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, consultez [Abonnement 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, consultez [Lancement 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, consultez [Lancement 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 dans AWS 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 la section [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 ECS, EKS 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 Anywhere est 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.

### Exemple 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 dans AWS 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 Manager aide de votre Compte 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 à AWS 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 conteneur AWS 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. Dans AWS 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 dans AWS 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 qui contient 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 dans AWS Marketplace, voir [Rechercher 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'avez 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, consultez [Options 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 produit AWS 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, voir [QuickLaunch 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 Anywhere](#) ou 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 Launch on a new EKS cluster with 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, consultez [QuickLaunch 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 Marketplace utilise 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 AWS endroit 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 dans [Lancement 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 AWS ressources que vous pouvez gérer comme

une seule unité. Toutes les ressources d'une pile sont définies par le CloudFormation modèle de la pile. 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 piles AWS CloudFormation, consultez la section [Utilisation des piles](#) dans le Guide de l'AWS CloudFormation utilisateur.

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 comporte une catégorie de produits d'apprentissage automatique auxquels vous pouvez vous abonner 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.

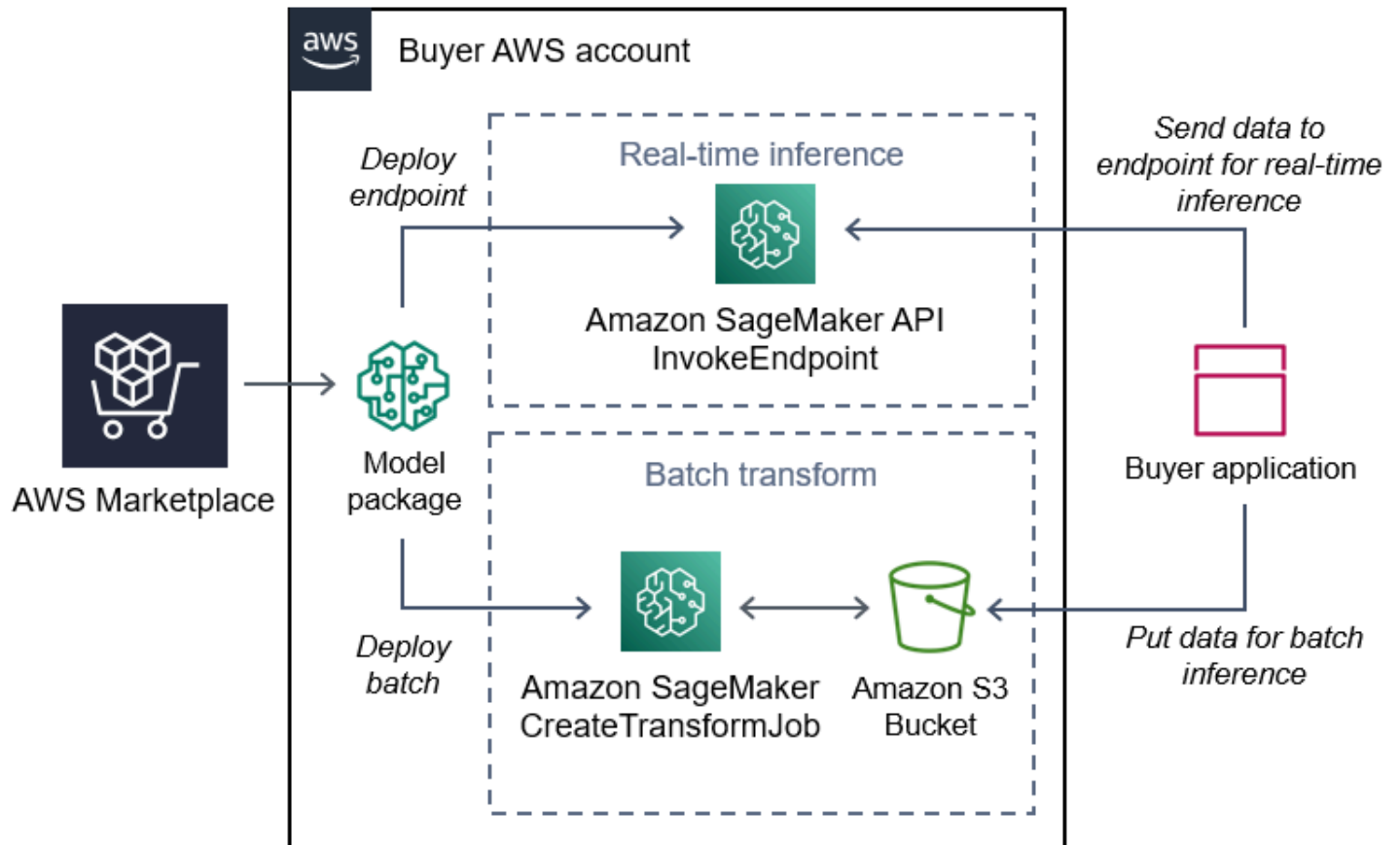
Pour évaluer la qualité et la pertinence d'un modèle, vous pouvez consulter les descriptions de produit, les instructions d'utilisation, les avis des clients, des exemples de [bloc-notes Jupyter](#), la tarification et les informations de support. Vous déployez des modèles directement depuis la SageMaker 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 SageMaker modèle de package Amazon est un modèle de machine learning unique préentraîné qui est 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 sur Amazon. SageMaker

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

1. Le AWS 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.



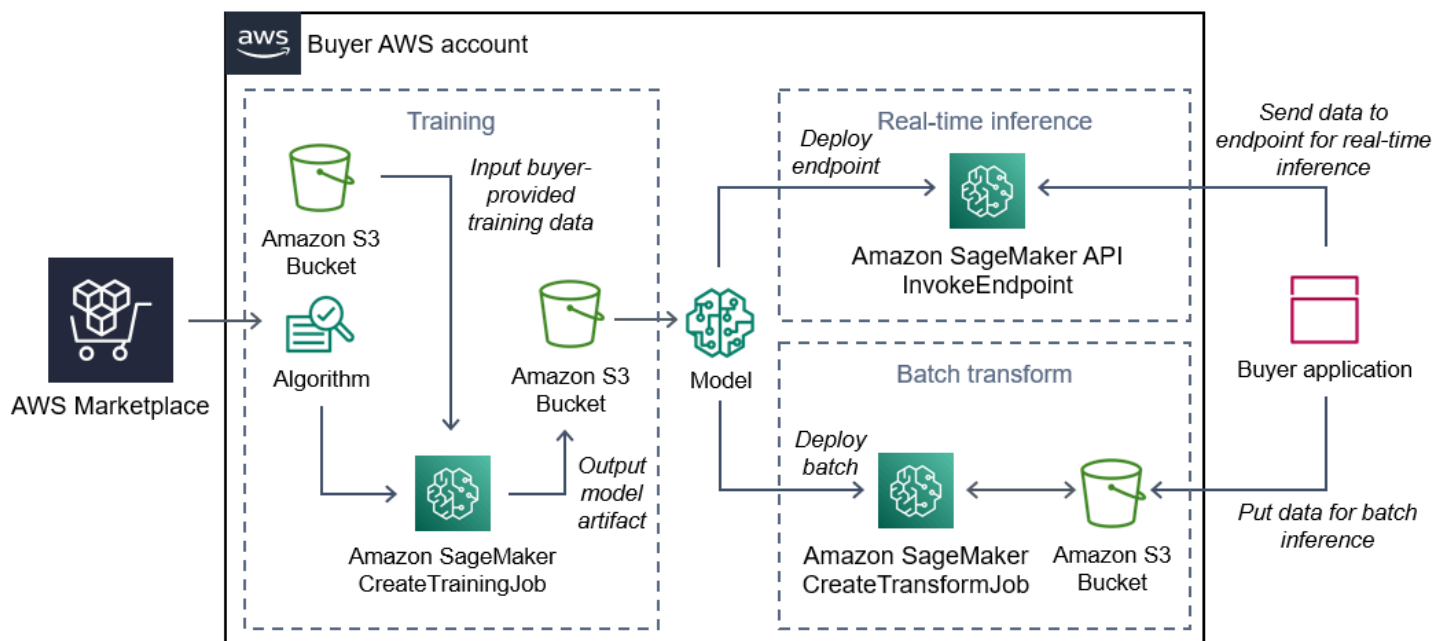
## SageMaker Algorithme Amazon

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. Le AWS 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 de machine learning.

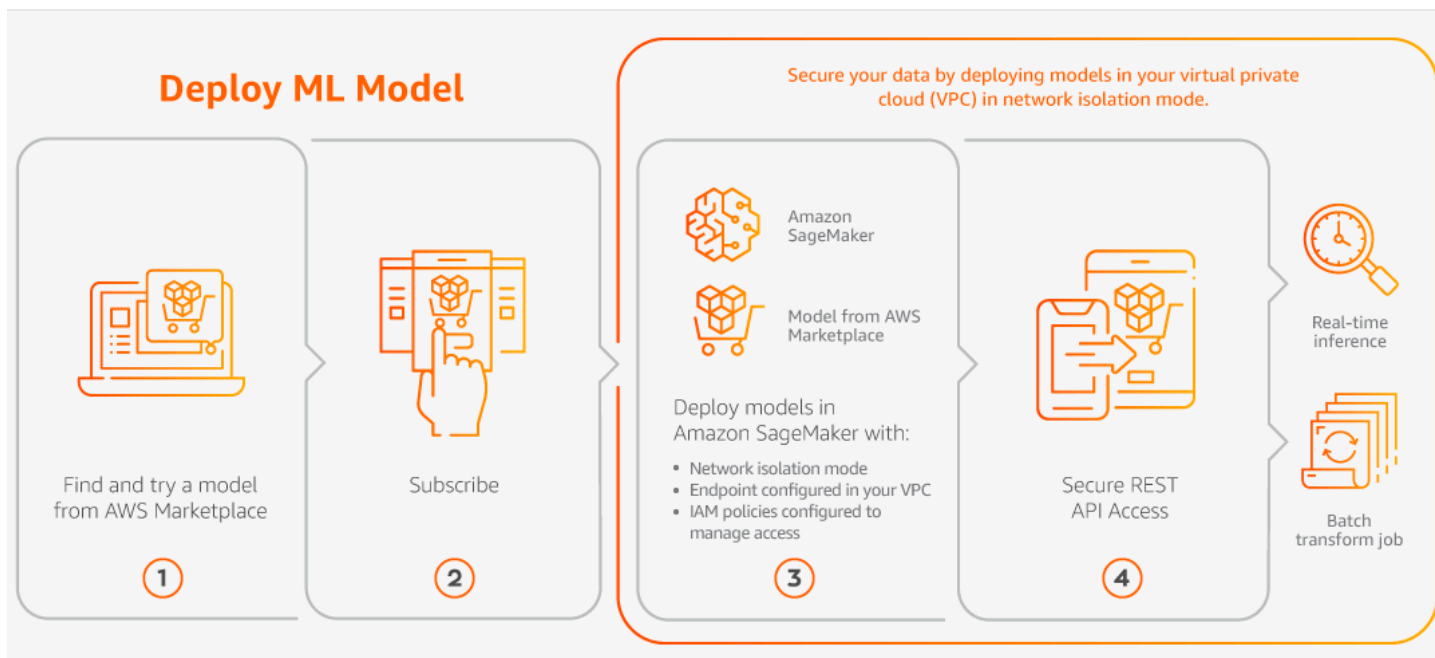
3. Lorsque le composant de formation du produit est terminé, il génère les artefacts du modèle d'apprentissage automatique.
4. SageMaker enregistre les artefacts du modèle dans votre compartiment Amazon Simple Storage Service (Amazon S3).
5. Dans SageMaker, vous pouvez ensuite déployer le composant d'inférence 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 sur 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 Marketplace fournit une facture consolidée pour les algorithmes et les packages de modèles, ainsi que les frais d'utilisation de l' AWS infrastructure.

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 d'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 Marketplace inclut des produits qui sont des services professionnels fournis par des AWS Marketplace vendeurs. Vous pouvez trouver ces produits dans la catégorie Services professionnels lorsque vous effectuez une recherche AWS Marketplace. Vous vous abonnez et achetez ces produits par le biais du vendeur AWS Marketplace, mais vous travaillerez avec le vendeur pour configurer les services professionnels répondant à vos besoins.

## Achat de services professionnels

Vous pouvez rechercher des services professionnels à l'aide de la catégorie Services professionnels dans AWS Marketplace. Lorsque vous trouvez un produit qui vous intéresse, demandez une offre au vendeur. Les services professionnels impliquant généralement une collaboration, vous devez fournir des 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. Accédez à votre AWS compte [AWS Marketplace](#) et connectez-vous, puis recherchez et trouvez le produit de services professionnels que vous souhaitez acheter.
2. Sur la page de détails du produit, sélectionnez Continuer.
3. Sur la page Demander un service, ajoutez les informations supplémentaires requises pour que le vendeur puisse créer l'offre, notamment votre nom, votre adresse e-mail, le nom de l'entreprise et toute information supplémentaire susceptible d'être utile au vendeur, notamment les besoins commerciaux, les délais et les exigences contractuelles.
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 AWS Marketplace. Ouvrez le lien dans un navigateur et connectez-vous à votre AWS compte.
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. Sous Configurer le contrat, choisissez la configuration que vous souhaitez utiliser pour votre contrat. Par exemple, si vous achetez un contrat d'assistance, il peut y avoir des options pour les contrats Silver, Gold ou Platinum, avec des prix différents.
7. Sélectionnez Créer un contrat pour acheter le service. Le vendeur doit vous contacter dans les 2 jours ouvrables pour vous fournir les instructions relatives à l'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 logiciels AWS Marketplace, mais vous accédez au produit dans l'environnement du vendeur de logiciels.

### Rubriques

- [Modèles de tarification](#)
- [Lancement rapide](#)

## Modèles de tarification

AWS Marketplace propose 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 autres Services 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 votre Compte 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, consultez [the 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 la configuration de votre compte et la vérification du paiement, vous verrez que votre contrat est en attente sur la page de AWS Marketplace détails 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 avez achetés AWS Marketplace sous 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 AWS est 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 dans AWS Secrets Manager, en votre nom.
- `DescribeSecrets`— Permet d' AWS Marketplace obtenir 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 Marketplace obtenir 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 l'utiliser AWS Marketplace pour rechercher des produits de données disponibles via AWS Data Exchange et vous y abonner. Pour plus d'informations, consultez la section [Abonnement aux produits de données sur AWS Data Exchange](#) dans le guide de l'utilisateur d'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'AWS infrastructure 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 Compte AWS résidez 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 Si vous Compte AWS résidez en Australie, vous recevez une facture d'Amazon Web Services Australia Pty Ltd (AWS Australia). Si vous Compte AWS résidez au Japon, vous recevez une facture d'Amazon Web Services Japan G.K (AWS Japan). Sinon, vous recevrez une facture de AWS Inc.

### Note

Pour les achats annuels et contractuels d'AMI, la facture des frais d'abonnement est facturée au moment de l'abonnement, plutôt que dans la facture mensuelle consolidée. Les achats annuels d'AMI génèrent une facture unique pour l'ensemble du contrat qui couvre tous les types d'instances achetés pendant l'abonnement. Les paiements flexibles sur les contrats sont facturés au moment du paiement prévu. Pour les contrats comportant des éléments d'utilisation (tels qu'un pay-as-you-go modèle), l'utilisation apparaît dans votre facture mensuelle consolidée.

AWS Marketplace les produits utilisant des topologies complexes peuvent entraîner des frais pour les clusters d'AMI et autres services d'AWS infrastructure lancés à l'aide du modèle fourni AWS 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 USD par heure et les frais EC2 de 0,085 USD par heure. À la fin du mois, vous êtes facturé 147,60 USD.

Pour plus d'informations sur l'abonnement aux produits de données, consultez la section [Abonnement aux 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 (AWS Europe), consultez [la section Gestion de vos paiements AWSEurope dans](#) le guide de l'AWS Billing utilisateur.

## Rubriques

- [Bons de commande](#)
- [Informations sur les remboursements](#)
- [Annuler l'abonnement à votre produit](#)
- [Moyens de paiement](#)
- [Devises supportées](#)
- [Modifier votre devise préférée](#)
- [Mise à jour des instructions de versement](#)

## Bons de commande

Lorsque vous utilisez des bons de commande dans AWS Marketplace et dans 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. Dans AWS 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 ultérieures 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 de serveur (y compris les instances AMI, les conteneurs, les AWS CloudFormation modèles et les graphiques Helm) avec un modèle de tarification annuel ou contractuel

**Note**

Le support 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 annuelle 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 dans AWS Marketplace, le compte de gestion de votre AWS organisation doit activer l' AWS Billing intégration. Cette tâche de configuration unique crée un rôle lié à un service, qui permet aux comptes de votre organisation autorisés à s'abonner d'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. Trouvez un [produit compatible](#) et préparez-vous à l'acheter auprès de AWS Marketplace.
2. Pendant le processus d'achat, sur la page Configurer votre abonnement logiciel (pour le SaaS), dans 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.

Votre numéro de 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 comporter 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 pour l'utilisation de couvertures

Pour séparer les AWS Marketplace frais des autres bons de commande, vous pouvez créer un bon de commande avec une rubrique d'utilisation AWS Marketplace générale dans la AWS Billing console. AWS Marketplace les transactions de facturation incluront le bon de commande global que vous spécifiez si certains critères et paramètres correspondent (par exemple, les entités de facturation). Les out-of-cycle factures qui ont spécifié un bon de commande AWS Marketplace transactionnel 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 <code>aws-marketplace:Subscribe</code> autorisé à vous abonner. Le compte de gestion doit également permettre l'AWS Billing intégration. Pour plus d'informations sur l'activation de l'intégration, consultez la section <a href="#">Création d'un rôle lié à un service</a> pour AWS Marketplace
Le bon de commande n'existe pas	AWS Marketplace crée 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 informations de contact (y compris les bons de commande créés par AWS 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 <a href="#">bord</a>

Scénario	Détails
	<a href="#">Purchase Orders de la console Billing and Cost Management.</a>
Numéro de bon de commande ajouté incorrect	Si vous avez saisi un numéro de bon de commande incorrect et que vous devez le mettre AWS Support à jour, contactez-nous pour le mettre à jour.
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 passe d'une organisation à l'autre, les nouvelles factures indiquent le numéro de bon de commande de 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 Billing intégration n'est disponible que pour les contrats SaaS, les produits de services 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	<p>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.</p> <p>Envisagez d'ajouter un bon de commande avec une <a href="#">rubrique d'utilisation AWS Marketplace générale</a> dans la AWS Billing console.</p>
Bon de commande suspendu	<p>Lorsqu'un numéro de bon de commande est fourni et que celui-ci est marqué comme suspendu dans le tableau de bord Purchase Orders de la console Billing and Cost Management, le nouveau poste est ajouté 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.</p>
Bon de commande expiré	<p>Lorsqu'un numéro de bon de commande est fourni et que le bon de commande est expiré, le nouveau poste est créé et le bon de commande est marqué comme actif. La date de fin de l'article est utilisée comme date d'expiration du nouveau bon de commande.</p>
Suivi du solde	<p>Le suivi du solde n'est pas activé pour les AWS Marketplace rubriques.</p>
Intégration du système d'approvisionnement	<p>Le bon de commande fourni par un système d'approvisionnement intégré apparaît sur les factures.</p>

Scénario	Détails
Calendrier de paiement flexible - achat initial	Un contrat comportant des dates de facturation spécifiques (calendrier de paiement flexible) génère un premier article 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 sur les différents bons de commande, contactez-nous AWS Support pour modifier le numéro de bon de commande sur les futures factures.

## Informations sur les remboursements

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

Pour plus d'informations sur les remboursements liés à vos AWS Marketplace achats, consultez les rubriques suivantes du Guide du AWS Marketplace vendeur :

- [Remboursements](#)
- [Tarification du produit](#)

### Note

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

## Annuler l'abonnement à votre produit

Vous pouvez annuler votre abonnement au produit ou le renouveler automatiquement dans AWS Marketplace. Les étapes suivantes fournissent des instructions pour les produits Software as a Service (SaaS), Machine Learning (ML) et Amazon Machine Image (AMI) dans AWS Marketplace.

### Rubriques

- [Résiliez votre abonnement SaaS](#)
- [Annulation de votre abonnement au machine learning](#)
- [Annulation de votre abonnement AMI](#)
- [Annuler le renouvellement automatique de votre abonnement au contrat SaaS](#)

## Résiliez votre abonnement SaaS

1. Connectez-vous à la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 au machine learning

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

- Pour les algorithmes ML, connectez-vous à la SageMaker console [Amazon AWS 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 un point de terminaison en temps réel ou créer une tâche d'inférence par lots après l'annulation de votre abonnement au machine learning.
- Pour les packages de modèles ML ou les modèles créés à partir de vos algorithmes, connectez-vous à la SageMaker console [Amazon AWS Management Console et ouvrez-la](#). Mettez fin à tous les points de terminaison en temps réel en cours d'exécution pour vos modèles ou à toutes les tâches d'inférence par lots en cours d'exécution.



**Note**

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

Pour annuler un abonnement à l'apprentissage automatique

1. Connectez-vous à la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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. Ouvrez Gérer dans AWS 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 mettre hors service. Vous devez également supprimer les AWS CloudFormation piles, le cas échéant.
9. Retournez 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 vous sera plus facturé.

## Annuler le renouvellement automatique de votre abonnement au contrat SaaS

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

## Moyens de paiement

Lorsque vous avez créé votre compte Compte AWS, vous avez défini le mode de paiement pour ce compte. Vous pouvez gérer vos méthodes 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 survient lors du traitement de votre paiement via votre compte payeur, mettez à jour votre mode de paiement et réessayez. Des erreurs peuvent survenir pour les raisons suivantes :

- Le mode de paiement est manquant, non valide ou n'est pas pris en charge.
- Le paiement a été refusé.
- Votre compte Amazon Internet Services Private Limited (AISPL) limite l'utilisation de 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 des achats par carte de crédit et de débit pour les clients de l'AISPL AWS Marketplace sur 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 le dépannage, contactez [AWS Support](#).

## Devises supportées

Les listes suivantes incluent toutes les devises prises en charge pour AWS Amazon Web Services EMEA SARL, Amazon Web Services Australia et Amazon Web Services Japan G.K.

### Note

La roupie indienne (INR) n'est pas prise en charge car Amazon Internet Services Private Limited (AISPL) n'est actuellement pas prise en charge sur AWS Marketplace. Pour plus d'informations, voir [Quelles sont les différences entre les comptes AISPL 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)
- Euros (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)

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

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

- Dollar australien (AUD)
- Dollar américain (USD)

Les devises prises en charge par Amazon Web Services Japan G.K. sont les suivantes :

- Yen japonais (JPY)
- Dollar américain (USD)

## Modifier votre devise préférée

Vos AWS Marketplace achats sont affichés dans la devise que vous avez spécifiée pour votre Compte AWS. Vous pouvez modifier la devise préférée de votre compte dans la [AWS Billing and Cost Management console](#). 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 des paramètres du compte dans la AWS Billing and Cost Management console.](#)

## Mise à jour des 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 d'Amazon Web Services EMEA SARL \(AWS Europe\) contiennent des instructions de paiement différentes de celles de AWS, Inc. Vous pouvez trouver les 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 des informations de versement de la facture sont différents des achats de services par le biais d'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 effectuant des transactions	Instructions de versement
AWS Cloud achats de services	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
AWS Marketplace Vendeur éligible	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
Vendeur non éligible AWS Marketplace	AWS Inc.	AWS

<Pour demander une lettre bancaire contenant les instructions de versement, sélectionnez

Pour plus d'informations sur la façon de modifier votre préférence de devise pour 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 fonds MasterCard, par carte 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 Marketplace l'aide fiscale pour les acheteurs](#).

# Balisage de répartition des coûts

AWS Marketplace prend en charge le balisage de répartition des coûts pour les produits logiciels que vous achetez. Vous pouvez utiliser les balises de répartition des coûts activées pour identifier et suivre l'utilisation AWS Marketplace des ressources par le biais AWS Cost Explorer de rapports sur les AWS coûts et d'utilisation, de AWS budgets ou d'autres outils d'analyse des coûts du cloud. Pour faciliter la catégorisation et le suivi de vos AWS Marketplace coûts, vous pouvez utiliser des balises de répartition des coûts pour organiser les coûts des ressources dans votre rapport de répartition des coûts.

Les étiquettes de répartition des coûts AWS Marketplace proviennent des deux sources suivantes :

- Les coûts des produits logiciels Amazon Machine Image (AMI) associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) dotée de balises héritent de ces mêmes balises. Vous pouvez activer ces balises en tant que balises de répartition des coûts dans la AWS Billing and Cost Management console d'un compte. Pour plus d'informations sur l'utilisation des balises de répartition des coûts avec les produits AMI, consultez [Étiquetage de répartition des coûts dans les produits AMI](#).
- Les produits AMI, conteneur et logiciel 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 peut utiliser une balise pour identifier l'utilisation par département. Pour plus d'informations sur l'utilisation de ces balises, consultez [Étiquettes mesurées par le fournisseur](#).

Le balisage de répartition des coûts permet de suivre les coûts uniquement à partir du moment où les balises ont été activées dans la console Billing and Cost Management. Seuls Compte AWS les propriétaires, les propriétaires de comptes de AWS Organizations gestion et les utilisateurs disposant des autorisations appropriées peuvent accéder à la console Billing and Cost Management pour un compte. Que vous utilisiez ou non le balisage de répartition des coûts, le montant qui vous est facturé ne change pas. L'utilisation de balises de répartition des coûts n'a aucune incidence sur les fonctionnalités de vos produits AWS Marketplace logiciels.

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

## Étiquettes mesurées par le fournisseur

AWS Marketplace les produits dotés d'un système de mesure du fournisseur (notamment les produits AMI, les conteneurs et les produits SaaS) peuvent être dotés de balises fournies par le fournisseur du logiciel 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 vos AWS Marketplace ressources selon les indicateurs fournis par le fournisseur. Vous pouvez utiliser ces balises pour identifier et suivre l'utilisation AWS Marketplace des ressources via AWS Cost Explorer Service, AWS Cost and Usage Report AWS Budgets, ou d'autres outils d'analyse des coûts du cloud.

Les balises apparaissent dans votre AWS Billing console lorsque vous commencez à utiliser le AWS Marketplace produit et que le fournisseur envoie les relevés de mesure à AWS Marketplace. Si vous utilisez un produit sur la base d'un engagement initial stipulé dans un contrat, vous ne recevrez pas de comptage pour le produit. Par conséquent, vous n'aurez pas les balises définies par le fournisseur dans votre console. AWS Billing Si vous gérez un compte associé, vous devez disposer à la fois des ViewBilling autorisations ModifyBilling et des autorisations pour afficher et activer les tags AWS Billing. Pour plus d'informations, consultez les [politiques relatives aux actions de facturation AWS](#) dans le guide de l'utilisateur d'AWS Billing.

### Note

L'activation de 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 liés à Amazon S3 pourraient également augmenter.

Pour activer les tags mesurés par le fournisseur pour tous les produits éligibles AWS Marketplace

1. Connectez-vous à la [AWS Billing console AWS Management Console et ouvrez-la](#). Choisissez ensuite les balises de répartition des coûts dans le volet de navigation de gauche.
2. Choisissez l'onglet balises de répartition des coûts AWS générées par -generated.
3. Recherchez pour `aws:marketplace:isv:` trouver des balises pour tous les produits qui prennent en charge le balisage mesuré par le fournisseur.
4. Cochez les cases correspondant à tous les tags, puis choisissez 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](#) de l'utilisateur AWS Billing

# Places de marché privées

Un marché privé contrôle les produits auprès desquels les utilisateurs de votre entreprise Compte AWS, tels que les utilisateurs professionnels et les équipes d'ingénierie, peuvent se procurer AWS 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 disponibles AWS 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, consultez [Création 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 de Services 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 approuvé AWS 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 public AWS 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 `AWSPivateMarketplaceAdminFullAccess` IAM. Pour plus d'informations sur l'application de cette politique aux utilisateurs, aux groupes et aux rôles, consultez [the 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 `AWSPivateMarketplaceAdminFullAccess` 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 du AWS Marketplace Catalog API. Pour plus d'informations, consultez la section [Travailler avec un marché privé](#) dans la AWS Marketplace Catalog API référence.

## 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 pour AWS 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 pour AWS 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 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 avec AWS 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 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 régir 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 depuis 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 AWS Private 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 public AWS 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 public AWS 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 sur le 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 grâce à 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 les prix et les conditions avec le vendeur, qui crée une offre privée pour le AWS compte que vous désignez. 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 dans AWS 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 Marketplace les 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 utiliser la facturation détaillée pour consulter votre consommation pour chacun des produits que vous

AWS Marketplace avez achetés. 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 tous vos abonnements logiciels annuels dans la AWS Marketplace section 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 <a href="#">Acceptation d'une offre privée</a> dans le guide de l'utilisateur d'AWS Data Exchange.
Contrat SaaS	<p>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.</p> <p>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.</p> <p>Le vendeur peut également inclure des pay-as-you-go prix négociés pour une utilisation supérieure à l'utilisation prévue dans le contrat.</p>
Abonnement SaaS	Avec un abonnement SaaS, vous acceptez un prix pour l'utilisation d'un produit. Le vendeur assure le suivi de votre consommation et vous



Type d'offre	Description
	en AWS Marketplace informe, et vous êtes facturé pour ce que vous consommez.
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'informations, consultez <a href="#">Produits de services professionnels</a> .

## 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 AWS facturation et vos paramètres fiscaux.

### Note

Certains vendeurs offrent la possibilité de demander une offre privée pour leur produit sur AWS Marketplace. Pour les vendeurs participants, un bouton Demander une offre privée s'affichera sur la page détaillée du produit. Pour demander une offre privée, cliquez sur le bouton et fournissez les détails de la demande. Vous recevrez un e-mail de confirmation résumant votre demande, et un AWS représentant vous contactera.

## 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/](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 consulter ou modifier vos paramètres fiscaux, connectez-vous au AWS Management Console

et, dans les paramètres de votre compte, consultez les paramètres fiscaux. 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'un lien fourni par le vendeur](#)
- [Consulter et souscrire à une offre privée depuis la page du produit](#)

## 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 [AWS Marketplace](#) console.
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 [AWS Marketplace](#) console.
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 [AWS Marketplace](#) console.
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 privées AWS 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 correctement Compte 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 AWS identifiant 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, consultez [Sécurité activée 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'utiliser Internet 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

Dans AWS 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, consultez [Modification 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 pour AWS Marketplace, consultez [AWS politiques 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 votre Comptes 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.

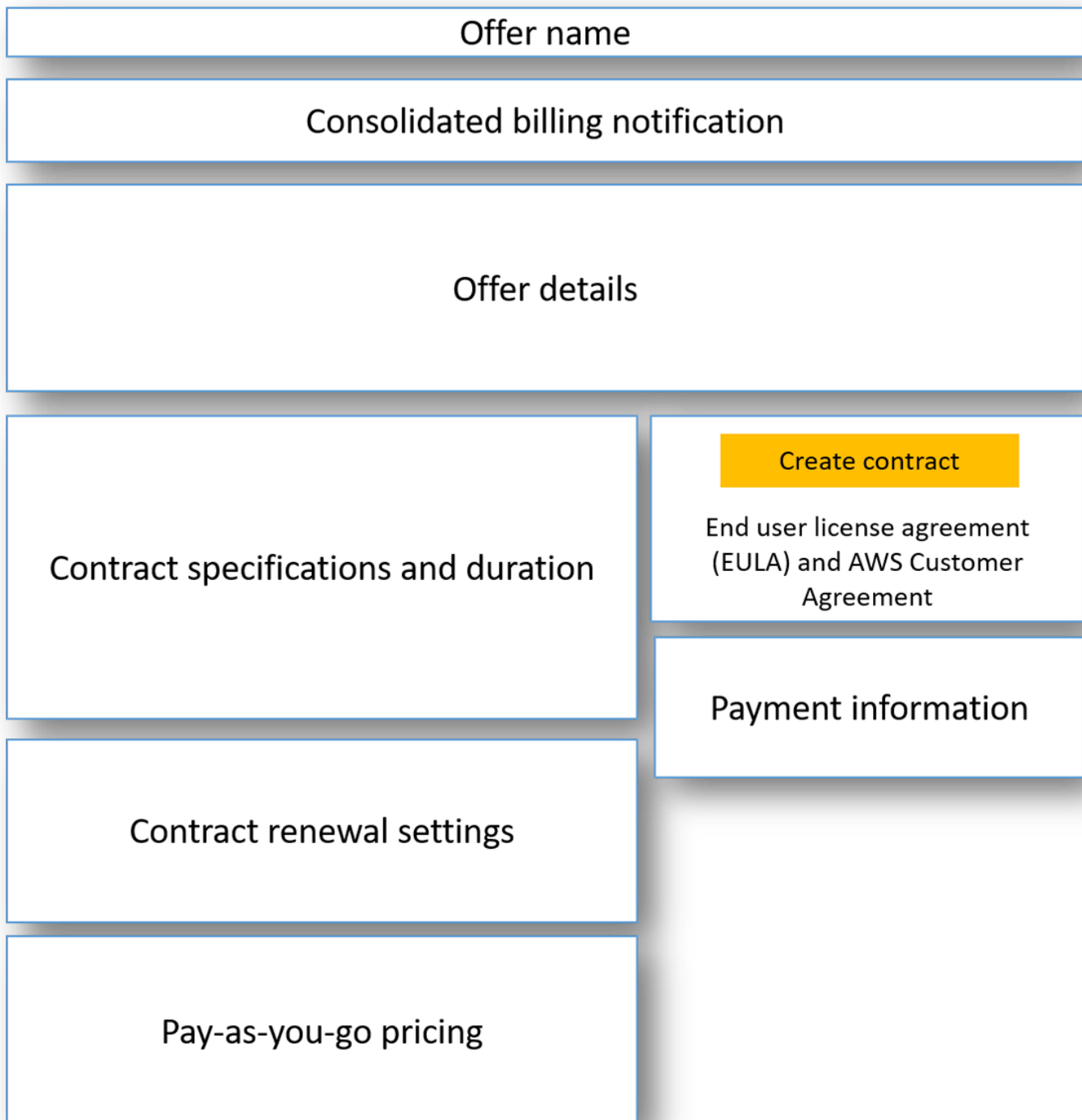
 Note

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 pour [Affichage 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 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 le AWS Marketplace site Web.

Comme le montre le schéma 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 concerné par l'offre privée. 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 contient 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 le 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 au prix de l'instance que vous avez négocié, 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 sa date de fin.
- **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.

#### Note

Si vous ne parvenez pas à accéder à un type d'instance ou Région AWS s'il n'était peut-être pas pris en charge au moment où l'offre privée vous a été envoyée. Consultez les détails de votre contrat pour plus d'informations. Pour accéder à une instance ou à une région, contactez le vendeur et demandez une offre privée actualisée. Après avoir accepté la nouvelle offre, vous aurez accès à l'instance ou à la région nouvellement ajoutée.

Vendor name and product Continue to Configuration button

Page guidance

Terms and Conditions

Private offer name Private Offer

Notification for accepting the private offer contract Accept Contract button

Contract duration

Components included in the contract

Additional usage costs

Terms duration

Additional offer information

Contract pricing

Scheduled payments

Other Available Offers


## Souscrire 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 le AWS Marketplace site Web. Vous ne pouvez pas accepter l'offre privée sur la AWS Marketplace console ou sur la 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 sur 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 pour [Affichage d'une offre privée et abonnement](#).

2. Assurez-vous de consulter l'offre privée adéquate. Le vendeur peut créer plusieurs offres privées pour vous 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 que c'est bien 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

N'actualisez pas votre navigateur pendant que le système traite la demande de 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.

## Souscrire 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 le AWS Marketplace site Web. Vous ne pouvez pas l'accepter sur la AWS Marketplace console ou sur la console Amazon EC2. 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. Pour accepter une offre privée AMI sans calendrier de paiement flexible, suivez la procédure suivante.

Pour accepter une offre privée AMI sans calendrier de paiement flexible

1. Assurez-vous de consulter l'offre privée adéquate. Le vendeur peut créer plusieurs offres privées pour vous 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 comme étant en train de consulter 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 que c'est bien 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, pour Type d'instance, choisissez dans la liste des types d'instance disponibles. Pour Quantité, choisissez le nombre de licences.
7. Passez en revue 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 dans AWS 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 autre Compte 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 vigueur AWS 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](#)
- [Utilisation d'un planificateur de paiement flexible avec des accords futurs](#)
- [Modification de vos futurs contrats](#)
- [Réception de notifications concernant de futurs accords datés](#)

## 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 pour [Affichage 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 AWS Marketplace, un accord est créé qui vous accorde une licence d'utilisation de ces produits. Si vous Compte AWS êtes membre d'une organisation, vous pouvez partager cette licence pour Amazon Machine Image (AMI), les conteneurs, le machine learning et les produits de données avec les autres comptes de cette organisation. Vous devez configurer le support des licences dans AWS Marketplace, puis le partager depuis l'intérieur AWS License Manager.

## Note

Pour plus d'informations AWS Organizations, consultez le [guide de AWS Organizations l'utilisateur](#).

Pour plus d'informations sur le partage de licences avec votre organisation dans AWS License Manager, consultez la section [Licences accordées](#) dans le Guide de AWS License Manager l'utilisateur.

La vidéo suivante présente une présentation détaillée de l'expérience de partage de licences.

## [Répartissez vos droits de AWS Marketplace licence \(3:56\)](#)

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

### Rubriques

- [Conditions préalables au partage de licences](#)
- [Afficher vos licences](#)
- [Partage de vos licences](#)
- [Suivi de l'utilisation des licences](#)

## Conditions préalables au partage de licences

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

- Donnez AWS Marketplace l'autorisation de gérer les licences en votre nom afin qu'il puisse créer les licences associées lorsque vous achetez ou partagez vos licences. Pour plus d'informations, consultez [Utiliser des rôles pour partager des droits pour AWS Marketplace](#).
- Configuré AWS License Manager pour la première utilisation. Pour plus d'informations, consultez la section [Mise en route AWS License Manager](#) dans le guide de AWS License Manager l'utilisateur.

## Afficher vos licences

AWS Marketplace crée 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 les licences à l'aide de AWS License Manager. Toutefois, vous pouvez l'utiliser AWS Marketplace pour consulter les licences des produits que vous avez achetés auprès de ce site AWS Marketplace.

Pour consulter les licences des produits auxquels vous êtes abonné dans AWS 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 licences AWS Marketplace gérées dans la console License Manager.
  - Pour consulter les licences associées à un seul abonnement
    - a. Choisissez la fiche du produit que vous souhaitez consulter pour accéder à la 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, conteneur, machine learning et de données disposent de licences pouvant être partagées.

Les abonnements AWS 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 Marketplace soutient les subventions, qui partagent l'utilisation d'une licence directement avec AWS Organizations Compte AWS, une ou une unité organisationnelle utilisant AWS License Manager. Le processus d'activation des subventions inclut désormais des options supplémentaires pour remplacer les subventions activées pour le même produit d'origine AWS 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 des articles spécifiques Régions AWS, un compte avec lequel vous partagez votre licence ne peut activer la licence que s'il se trouve dans une région autorisée.

## Suivi de l'utilisation des licences

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



Pour plus d'informations sur l'utilisation de License Manager pour suivre l'utilisation de vos licences, consultez la section [Licences accordées](#) dans le guide de AWS License Manager l'utilisateur.

# Notifications aux acheteurs concernant les AWS Marketplace événements

AWS Marketplace fournit des notifications en temps opportun par e-mail, sur EventBridge les événements Amazon et sur 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'acheteur AWS 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 AWS identifiant de l'acheteur.

Certains fournisseurs de messagerie (par exemple, Google ou Yahoo) peuvent filtrer vos e-mails de notification AWS Marketplace. Si vous n'avez pas reçu de notifications de votre part AWS Marketplace ou si vous les voyez dans votre dossier de courrier indésirable, ajustez vos paramètres de messagerie. Consultez par exemple les [instructions du groupe Google](#) ou les [instructions de Yahoo](#).

# EventBridge Notifications Amazon pour les AWS Marketplace événements

AWS Marketplace est intégré à Amazon EventBridge, anciennement 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](#)

## 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	<a href="#">the section called “Événements pour les nouvelles annonces”</a>

## 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 AWS Marketplace aux systèmes d'approvisionnement

Vous pouvez configurer l'intégration de AWS Marketplace et de votre logiciel d'approvisionnement Coupa ou SAP Ariba. Une fois la configuration terminée, les utilisateurs de votre organisation peuvent utiliser votre logiciel d'approvisionnement pour rechercher et demander un abonnement aux AWS Marketplace produits. 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 AWS Marketplace, le produit logiciel est répertorié comme un abonnement acheté et peut être utilisé. L'intégration à votre système d'approvisionnement peut également 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, connu sous le nom de punchout.

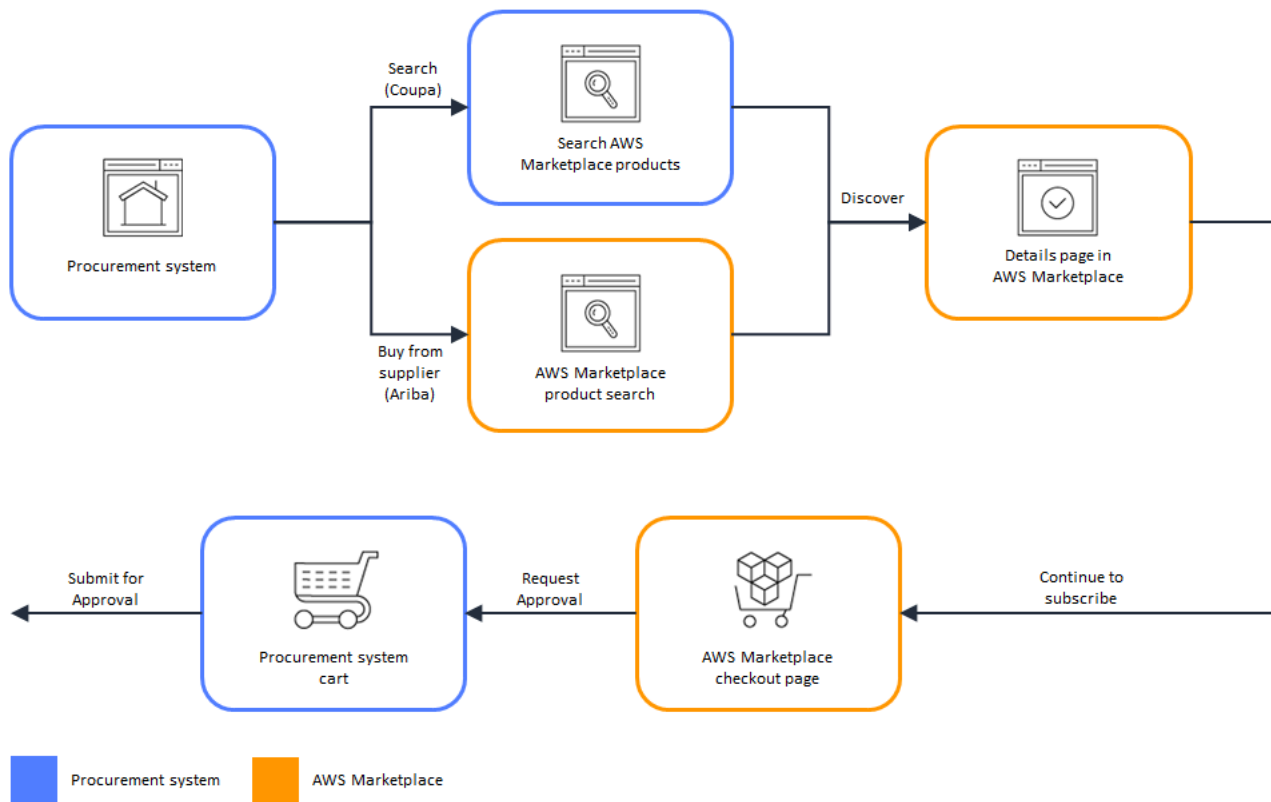
L'intégration varie légèrement en fonction du système d'approvisionnement :

- **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 vers le site AWS Marketplace pour 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 se lancer directement dans AWS Marketplace la recherche de produits.
- **SAP Ariba** — Ariba redirige les utilisateurs AWS Marketplace vers eux pour rechercher un logiciel et obtenir des informations sur un produit. Une fois qu'un administrateur a configuré l'intégration de Punchout, les utilisateurs du logiciel d'approvisionnement d'Ariba peuvent trouver le AWS Marketplace logiciel en choisissant l'onglet Catalogue, puis en sélectionnant le catalogue. AWS Marketplace Cela les redirige AWS Marketplace vers les produits qui les intéressent.

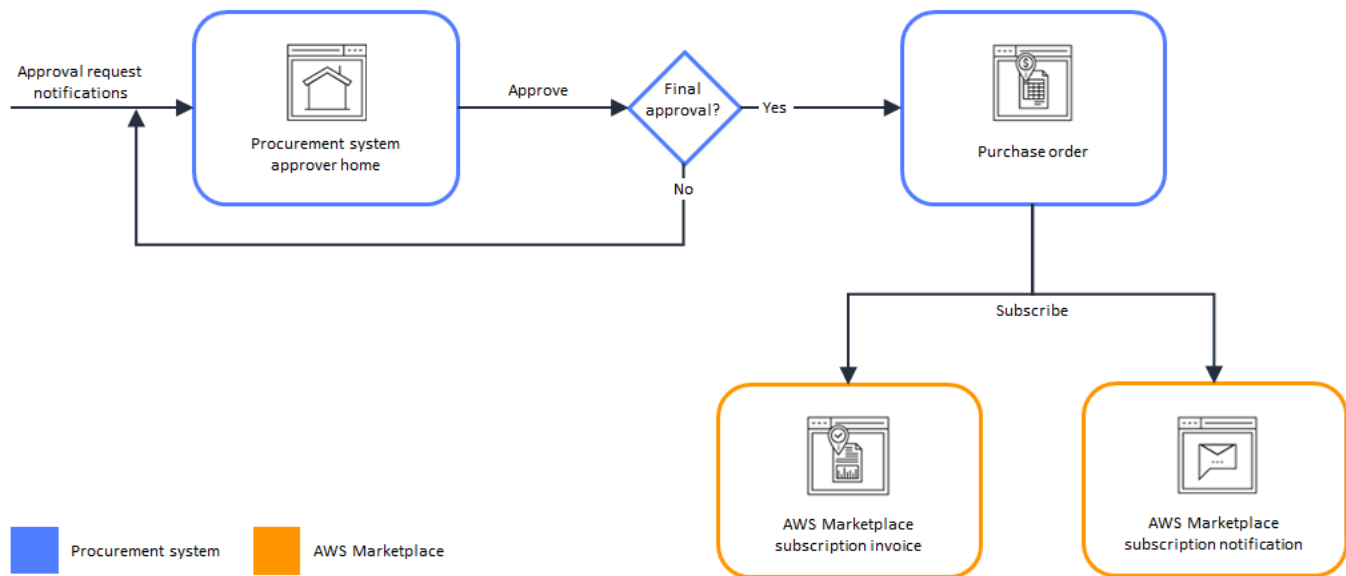
Les utilisateurs d'Ariba doivent effectuer leur achat depuis Ariba, et non. AWS Marketplace

Lorsque l'utilisateur souhaite acheter un abonnement dans lequel il navigue AWS Marketplace, il crée une demande d'abonnement dans celui-ci AWS Marketplace. Sur la page d'abonnement du produit,

au lieu de terminer l'achat, l'utilisateur demande l'approbation. La demande est renvoyée dans un panier d'achat dans le système d'approvisionnement pour terminer le processus d'approbation. Le schéma suivant montre le processus de demande d'abonnement au système d'approvisionnement.



Lorsque le système d'approvisionnement reçoit la demande AWS 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 retourner à pour AWS Marketplace finaliser l'achat. Cependant, ils voudront peut-être y retourner AWS Marketplace pour obtenir des instructions sur la façon d'utiliser le produit qu'ils ont acheté. AWS Marketplace envoie un e-mail au AWS compte utilisé pour accéder AWS Marketplace. Le message électronique informe le destinataire que l'abonnement a réussi et que le logiciel est disponible via AWS 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 incluent les suivantes :

- Les essais gratuits ne génèrent pas de facture dans le système d'approvisionnement, car ils ne sont pas payants.
- Les contrats comportant 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 utilisant le 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 leurs commandes à leur système d'approvisionnement pour approbation. Lorsque le paramètre est désactivé, les clients soumettent les 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 passées 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 démarrez le processus AWS Marketplace et vous le terminez 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 Compte AWS utilisé pour terminer la AWS Marketplace configuration doit être le compte de gestion 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 catalogue de contrats, de fournisseurs et de punchout dans le système d'approvisionnement.

## Configuration des autorisations IAM

Les autorisations IAM suivantes figurent dans la politique [AWS politique gérée : `AWSMarketplaceProcurementSystemAdminFullAccess`](#) gérée et sont requises pour configurer l'intégration entre un système d'approvisionnement 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 dans AWS Marketplace, consultez [Sécurité activée AWS Marketplace](#).

## Configuration AWS Marketplace en vue de l'intégration à Coupa

Après avoir 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 le nom et la description du punchout. Vous pouvez également passer l'intégration en mode test afin que les utilisateurs puissent tester l'intégration sans créer d'abonnement à des produits tant que vous n'êtes pas prêt. Pour configurer la AWS Marketplace partie de l'intégration, procédez comme suit.

Pour configurer en vue AWS Marketplace de l'intégration avec 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 souhaitez peut-être que vos factures dans la AWS Billing console fassent référence au bon de commande en langage de balisage extensible (cXML) utilisé pour souscrire à votre produit contractuel SaaS (Software as a Service). Si tel est le cas, vous pouvez activer l'intégration de facturation à l'aide d'un rôle lié au 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 l'intégration terminée AWS 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 par défaut indique que le mode test est activé. En mode test, les demandes d'abonnement sont envoyées au backend de 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 AWS Marketplace dans votre système Coupa, copiez les informations du volet Informations d'achat de la page Gérer l'intégration Coupa dans AWS Marketplace. Utilisez ces informations pour suivre les étapes indiquées 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 par AWS Marketplace, voir. [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 pour créer un punchout 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 :


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

 Note

Vous souhaitez peut-être que vos factures dans la AWS Billing console fassent référence au bon de commande cXML utilisé pour souscrire à votre produit de contrat SaaS. Si tel est le cas, vous pouvez activer l'intégration de facturation à l'aide d'un rôle lié au 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 Marketplace vous 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 avec AWS Marketplace.

En suivant les instructions et les paramètres de configuration de l' AWS Marketplace équipe, vous créez l'intégration dans votre environnement de test SAP Ariba, en l' AWS Marketplace exécutant en mode test. Dans l'environnement de test, les demandes d'abonnement sont envoyées au backend d'Ariba afin que vous puissiez voir le flux complet, y compris les approbations, sans créer d'abonnement AWS Marketplace, et aucune facture n'est générée. Cette approche permet de tester la configuration avant d'activer le punchout en production. Une fois que vos tests sont 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 créent des demandes, mais aucun logiciel ne sera acheté.

Lorsque vos tests sont terminés et que vous avez travaillé avec l' AWS Marketplace équipe 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 par AWS Marketplace, voir. [Codes UNSPSC utilisés par AWS Marketplace](#)

## Codes UNSPSC utilisés par AWS Marketplace

AWS Marketplace utilise le code des produits et services standard des Nations Unies (UNSPSC) 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 sur le AWS Marketplace côté, vous devez [nous contacter](#).

## Essais gratuits

Certains produits répertoriés AWS Marketplace proposent 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 à une durée spécifique. Vous ne pouvez pas suspendre une période d'essai gratuite une fois qu'elle commence.

## Tarification des logiciels et de l'infrastructure

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

### Note

Certains produits peuvent nécessiter une AWS infrastructure supplémentaire pour fonctionner. Par exemple, les vendeurs peuvent fournir des instructions de déploiement ou des modèles permettant de déployer des équilibreurs de charge, des solutions de stockage, des bases de données ou autres Services AWS dans votre Compte AWS. Pour comprendre ce que Services AWS le vendeur a demandé pour son produit, consultez les pages détaillées des produits répertoriés sur le site AWS Marketplace. Ensuite, consultez les pages de tarification de ceux-ci Services AWS.

## Essais gratuits pour les produits basés sur l'AMI

Certains produits AMI proposés à l'heure ou à l'heure avec une tarification annuelle AWS Marketplace proposent des essais gratuits. Lorsque vous souscrivez à un essai gratuit, vous pouvez exécuter une instance Amazon EC2 du produit AMI pendant une durée définie par le vendeur sans encourir 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 abonnement payant à leur 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 la tarification [d'Amazon EC2](#).

## Essais gratuits pour les produits en conteneur

Certains produits en conteneur proposés à l'heure ou à l'heure avec une tarification à long terme AWS Marketplace font l'objet d'essais gratuits. Lorsque vous souscrivez à un essai gratuit, vous pouvez exécuter plusieurs tâches Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS) pendant un certain temps sans 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 par module. Les essais gratuits sont automatiquement convertis en abonnement payant à leur 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 toute utilisation continue entraîne des frais logiciels. Pour plus d'informations sur les frais d'infrastructure, consultez [les tarifs Amazon ECS](#) et [Amazon EKS](#).

## Essais gratuits pour les produits d'apprentissage automatique

Certains produits d'apprentissage automatique proposés à l'heure AWS Marketplace proposent des essais gratuits. Lorsque vous souscrivez à un essai gratuit, vous pouvez exécuter des SageMaker points de terminaison Amazon, des tâches de transformation par lots ou des tâches de formation pendant une durée définie par le vendeur sans avoir à payer les frais logiciels horaires. Vous êtes responsable des frais d'infrastructure. Les essais gratuits sont automatiquement convertis en abonnement payant à leur expiration.

Si vous ne résiliez aucun SageMaker point de terminaison Amazon, aucune tâche de transformation par lots ou aucune tâche 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 devez payer des frais logiciels pour toute utilisation continue. Pour plus d'informations sur les frais d'infrastructure, consultez [Amazon SageMaker Pricing](#).

## Essais gratuits pour les produits SaaS

Les produits Software as a service (SaaS) AWS Marketplace proposent des essais gratuits. Les essais gratuits du SaaS ne sont pas automatiquement convertis en contrats payants. Si vous ne souhaitez plus bénéficier de l'essai gratuit, vous pouvez le laisser expirer. Pour plus d'informations, voir [Essais gratuits de SaaS](#).



## Utilisation du niveau gratuit d'AWS avec AWS Marketplace.

Pour aider les nouveaux clients d'Amazon Web Services (AWS) à démarrer dans le cloud, AWS a introduit un niveau d'utilisation gratuit. 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. Lorsque la période d'utilisation gratuite expire (ou si l'utilisation de l'application dépasse les limites du niveau d'utilisation gratuite), vous payez simplement les tarifs de pay-as-you-go service standard. Pour de plus amples informations, veuillez consulter [Offre gratuite d'AWS](#).

Les clients d'AWS Free Tier peuvent utiliser gratuitement le logiciel AWS Marketplace pour un maximum de 750 heures d'utilisation d'Amazon Elastic Compute Cloud (Amazon EC2) par mois pendant un an. Consultez [AWS Marketplace](#) pour démarrer.

# Ajout d'abonnements AWS Marketplace à AWS Service Catalog

Service Catalog permet aux entreprises de créer et de gérer des catalogues de 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. 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 [Ajouter AWS 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 obtiennent les informations dont ils ont besoin pour faire des choix d'achat intelligents. En tant que client AWS, vous pouvez soumettre des commentaires écrits pour les articles répertoriés dans AWS 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 AWS Marketplace abonnée à un produit peut créer un avis pour celui-ci. Utilisez les instructions suivantes pour rédiger des avis sur les produits :

- Incluez 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 commentaires écrits doivent contenir au moins 20 mots et sont limités à 5 000 mots. La longueur idéale est de 75 à 500 mots.
- Soyez 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 clairement.

## Restrictions

AWS se réserve le droit de supprimer les avis contenant 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 avis sur les produits le plus rapidement possible. Cependant, l'AWS Marketplace équipe doit communiquer à la fois avec le réviser et le vendeur pour confirmer et vérifier la validité du commentaire par rapport à notre [the section called "Consignes"](#) et [the section called "Restrictions"](#). Nous suivons les mêmes directives en matière de [délais et d'attentes](#) que celles

décrites dans le Guide du AWS Marketplace vendeur en ce qui concerne le temps qu'il faudra pour terminer le processus.

## Obtention de support

Pour toute AWS Marketplace question d'ordre général, [contactez-nous](#). Pour toute question concernant le logiciel que vous achetez AWS Marketplace, contactez le vendeur du logiciel.

# AWS Marketplace Informations sur les fournisseurs

AWS Marketplace Vendor 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 Marketplace Vendor 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 à AWS 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 pour Services AWS.

AWS Marketplace Vendor 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 Manager capture 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 Marketplace Vendor Insights présente des informations de sécurité pour les produits logiciels disponibles dans AWS Marketplace. Vous pouvez utiliser AWS Marketplace Vendor Insights pour consulter les profils de sécurité des produits dans AWS 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, procédez comme suit.

Pour trouver des produits avec AWS Marketplace Vendor Insights

1. Connectez-vous à la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 Demande d'accès aux données Vendor Insights, 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 la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 Marketplace Vendor 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 Marketplace Vendor 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 la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
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 Marketplace Vendor 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, consultez [AWS Marketplace Informations sur les fournisseurs](#).

La liste suivante fournit une description de chaque catégorie de contrôle :

### Gestion des 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 gestion des accès](#)
- [Contrôles de sécurité des applications](#)
- [Contrôles d'audit et de conformité](#)
- [Contrôles de résilience de l'entreprise](#)

- [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.

Ensemble de contrôles	Titre du contrôle	Description du contrôle
Authentification sécurisée	Gestion des accès 3.1.1 - Authentification sécurisée - Entrée de données personnelles UserId (nécessite une attestation manuelle)	Avez-vous besoin de données personnelles (comme le nom ou l'adresse e-mail) de l'utilisateur ?
	Gestion des accès 3.1.2 - Authentification 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 - Authentification sécurisée - Verrouillage du compte (nécessite une attestation manuelle)	Le compte du client est-il verrouillé après 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 politique de mot de passe ?

Ensemble de contrôles	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 passe que les informations de connexion (nom d'utilisateur) soient cryptées et hachées avec du sel lors de leur
	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 sont-elles 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 à l'environnement de production ?
	Gestion des accès 3.3.2 - Accès à l'environnement de production - Authentification à deux facteurs	L'authentification à deux facteurs est-elle utilisée pour accéder à l'environnement de production 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 uniquement en cas d'exception pour accéder à l'environnement de production ?

Ensemble de contrôles	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'environnement est-il sécurisé à l'aide de mécanismes canaux cryptés ou une authentification ?
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 moindre privilège que les utilisateurs accèdent à l'environnement de 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'environnement de production sont-elles régulièrement révisées ?
	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 clients de créer des 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 logique de l'application ?
	Gestion des accès 3.4.5 - Politique de contrôle d'accès - Révision de l'accès en cas de résiliation	Toutes les politiques d'accès pertinentes sont-elles mises à jour lors du licenciement ou de la résiliation d'un rôle de l'employé ?



Ensemble de contrôles	Titre du contrôle	Description du contrôle
Journaux d'accès	Gestion des accès 3.5.1 - Journaux d'accès	Enregistrez-vous les activités effectuées par les utilisateurs individuels dans l'environnement de 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.

Ensemble de contrôles	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

Ensemble de contrôles	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

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	<p>Application Security 4.1.5 - Cycle de développement logiciel sécurisé - Image Backup</p>	<p>Les instantanés des images de l'application sont-ils sauvegardés ?</p>	<p>Spécifiez si les instantanés d'image (tels que les systèmes prenant en charge 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 ?</p>	<p>Oui. Les images sont sauvegardées avec l'approbation du client et de la direction.</p>

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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 par gravité.
	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.

Ensemble de contrôles	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

Ensemble de contrôles	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)	Stocker-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 PII 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



Ensemble de contrôles	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

Ensemble de contrôles	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 contrat de niveau de service 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.

Ensemble de contrôles	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	Dressez la liste des certifications que vous détenez.	Spécifiez les certifications que vous détenez.	SOC2, ISO/CEI 27001

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	attestation manuelle)			
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.

Ensemble de contrôles	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 réalisés 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.

Ensemble de contrôles	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

Ensemble de contrôles	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. Si oui, 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.

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	<p>Résilience et continuité des activités 6.1.3</p> <ul style="list-style-type: none"> <li>- Résilience des activités</li> <li>- Dépendances à l'égard de fournisseurs tiers (nécessite une attestation manuelle)</li> </ul>	<p>Existe-t-il des dépendances vis-à-vis de fournisseurs de services tiers essentiels (en plus d'un fournisseur de services cloud) ?</p>	<p>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 ?</p>	<p>Non</p>
	<p>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)</p>	<p>Exigez-vous que les fournisseurs tiers disposent de leurs propres processus et exercices de reprise après sinistre ?</p>	<p>Spécifiez si les fournisseurs tiers doivent disposer de leurs propres processus et exercices de reprise après sinistre.</p>	<p>Non applicable dans cet exemple.</p>

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	<p>Résilience et continuité des activités 6.1.5</p> <ul style="list-style-type: none"> <li>- Résilience des activités</li> <li>- Violation de contrat par des fournisseurs tiers (nécessite une attestation manuelle)</li> </ul>	<p>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) ?</p>	<p>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 ?</p>	<p>Non applicable dans cet exemple.</p>
	<p>Résilience et continuité des activités 6.1.6 - Résilience des activités - Health du système</p>	<p>Disposez-vous de moniteurs ou d'alertes pour évaluer l'état du système ?</p>	<p>Spécifiez si des moniteurs ou des alertes sont en place pour comprendre l'état du système.</p>	<p>Oui</p>

Ensemble de contrôles	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.



Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	<p>Résilience et continuité des activités 6.2.4</p> <p>- Continuité des activités - Impact sur la disponibilité dans les environnements multi-locataires (nécessite une attestation manuelle)</p>	<p>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 ?</p>	<p>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 ?</p>	<p>Oui. Seuil non disponible pour cet échantillon.</p>

Ensemble de contrôles	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

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
	<p>Résilience et continuité des activités 6.3.3</p> <p>- Disponibilité des applications - Portail des incidents en ligne (nécessite une attestation manuelle)</p>	<p>Existe-t-il un portail en ligne sur l'état de la réponse aux incidents qui décrit les interruptions planifiées et imprévues ?</p>	<p>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 ?</p>	<p>Oui. Le client peut accéder aux informations via exemple.com.</p>
	<p>Résilience et continuité des activités 6.3.4</p> <p>- Disponibilité des applications - Objectif de temps de restauration (nécessite une attestation manuelle)</p>	<p>Existe-t-il un objectif de temps de restauration (RTO) spécifique ?</p>	<p>Spécifiez s'il existe un objectif de temps de restauration (RTO). Si oui, pouvez-vous fournir le RTO ?</p>	<p>Oui, un RTO de 2 heures.</p>

Ensemble de contrôles	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.

Ensemble de contrôles	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 et Services AWS.

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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 fournirez des données clients.	Non

Ensemble de contrôles	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



Ensemble de contrôles	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

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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

Ensemble de contrôles	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. Si ce n'est pas le cas, expliquez les mécanismes dont vous disposez pour protéger les données contre la contamination croisée.	Oui

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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 ce problème 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.



Ensemble de contrôles	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.

Ensemble de contrôles	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

Ensemble de contrôles	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.

Ensemble de contrôles	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. Si non, comment appliquez-vous ce contrôle ?	Oui

Ensemble de contrôles	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.

Ensemble de contrôles	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

Ensemble de contrôles	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.

Ensemble de contrôles	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 une procédure 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. Dans l'affirmative, la vérification des antécédents est-elle effectuée régulièrement ?	Oui. La vérification des antécédents est effectuée chaque année.

Ensemble de contrôles	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.

Ensemble de contrôles	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



Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	Titre du contrôle	Description du contrôle	Détail de l'extraction des preuves	Valeur de l'échantillon
Services 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.

Ensemble de contrôles	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

Ensemble de contrôles	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 : <ul style="list-style-type: none"> <li>• Détails du problème identifié</li> <li>• Cause première</li> <li>• Commandes de compensation</li> <li>• Gravité</li> <li>• Propriétaire</li> <li>• Prochaines perspectives à court terme</li> <li>• La voie à suivre à long terme</li> </ul>

Ensemble de contrôles	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.

Ensemble de contrôles	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

Ensemble de contrôles	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.



Ensemble de contrôles	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

Ensemble de contrôles	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.

Ensemble de contrôles	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

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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.

Ensemble de contrôles	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 de AWS Marketplace Vendor Insights

Un instantané est point-in-time la posture 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 la [AWS Marketplace console AWS Management Console et ouvrez-la](#).
2. Choisissez Vendor Insights.
3. Dans Vendor Insights, choisissez un produit.
4. Dans l'onglet Sécurité et conformité, accédez à la section Résumé, puis choisissez Exporter.
5. Dans la liste déroulante, choisissez Télécharger (JSON) ou Télécharger (CSV).

## Contrôle de l'accès dans AWS Marketplace Vendor Insights

AWS Identity and Access Management (IAM) est un outil Service AWS qui vous permet de contrôler l'accès aux AWS ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires. Si vous êtes administrateur, vous contrôlez qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les AWS Marketplace ressources. AWS Marketplace Vendor Insights utilise l'IAM pour contrôler l'accès aux données des vendeurs, aux évaluations, à l'auto-attestation du vendeur et aux rapports d'audit conformes aux normes du secteur.

La méthode recommandée pour contrôler qui peut faire quoi Portail de gestion AWS Marketplace consiste à 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 à leur. Compte 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 faire AWS. Une politique autorise généralement l'accès à des actions spécifiques et peut éventuellement autoriser ces 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 chose Compte AWS. Toute modification apportée par un utilisateur peuvent avoir un impact sur l'ensemble du compte.

AWS Marketplace possède des autorisations définies pour contrôler les actions que peut effectuer une personne disposant de ces autorisations Portail de gestion AWS Marketplace. Il existe également des politiques qui AWS Marketplace créent et gèrent des politiques qui combinent 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, les ressources et les clés de condition disponibles, consultez la section [Actions, ressources et clés de condition pour AWS Marketplace Vendor Insights](#) dans la référence d'autorisation de service.

## Autorisations pour les acheteurs de AWS Marketplace Vendor Insights

Vous pouvez utiliser les autorisations suivantes dans les politiques IAM pour AWS Marketplace Vendor Insights. Vous pouvez combiner les autorisations au sein d'une seule politique IAM pour accorder les autorisations que vous souhaitez.

### **GetProfileAccessTerms**

GetProfileAccessTerms permet aux utilisateurs de récupérer les conditions nécessaires pour consulter, accepter et accéder à un profil AWS Marketplace Vendor Insights.

Groupes d'actions : lecture seule et lecture-écriture.

Ressources requises : SecurityProfile.

### **ListEntitledSecurityProfiles**

ListEntitledSecurityProfiles permet aux utilisateurs de répertorier tous les profils de sécurité qu'ils ont un droit de lecture actif.

Groupes d'actions : lecture seule, liste seule et lecture-écriture.

Ressources requises : Aucune

### **ListEntitledSecurityProfileSnapshots**

ListEntitledSecurityProfileSnapshots permet aux utilisateurs de répertorier les instantanés du profil de sécurité d'un profil de sécurité qu'ils ont un droit de lecture actif. 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 du profil de sécurité pour un profil de sécurité qu'ils ont un droit de lecture actif.



Groupes d'actions : lecture seule et lecture-écriture.

Ressources requises : SecurityProfile

# Sécurité activée 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 vendeurs AWS Marketplace, consultez [AWS Marketplace la 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 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 double adressage, vous devez vous assurer que toutes les politiques IAM utilisées pour le filtrage des adresses IP sont mises à jour pour inclure les plages d'adresses IPv6.

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'Conditionnement.

```
# 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'Conditionnement 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](#) de l'AWS Identity and Access Management utilisateur.

## Test du réseau après la mise à jour d'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 du AWS Marketplace site Web.

### Rubriques

- [Tester le réseau avec Linux/Unix ou Mac OS X](#)
- [Test du réseau avec Windows 7 ou Windows 10](#)
- [Tester le AWS Marketplace site](#)

### Tester le réseau avec Linux/Unix ou Mac OS X

Si vous utilisez Linux/Unix ou Mac OS X, vous pouvez vérifier si votre réseau accède 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
```

## Test du réseau avec Windows 7 ou Windows 10

Si vous utilisez Windows 7 ou Windows 10, vous pouvez vérifier si votre réseau peut accéder à un point de terminaison à double pile via IPv6 ou IPv4. Utilisez la commande ping, comme illustré dans l'exemple suivant.

```
ping aws.amazon.com
```

Cette commande renvoie les adresses IPv6 si vous accédez à un point de terminaison via IPv6.

## Tester le AWS Marketplace site

Le test des fonctionnalités du AWS 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 peuvent vous aider à commencer à tester les fonctionnalités du AWS Marketplace site Web.

En tant qu'acheteur sur le AWS Marketplace site Web, testez si vous pouvez effectuer les tâches suivantes :

- Abonnez-vous à un AWS Marketplace produit.
- Configurez un AWS Marketplace produit.
- Lancez ou commercialisez un AWS Marketplace produit.

En tant que vendeur sur le AWS Marketplace site Web, testez si vous pouvez effectuer les tâches suivantes :

- Gérez vos AWS Marketplace produits existants.

- Créez un AWS Marketplace produit.

## Contrôle de l'accès aux abonnements à AWS Marketplace

AWS IAM Identity Center vous permet de créer ou de connecter en toute sécurité les identités de vos employés et de gérer leur accès de manière centralisée pour toutes Comptes AWS les applications. L'IAM Identity Center est l'approche recommandée pour l'authentification et l'autorisation du personnel dans AWS les organisations de toutes tailles et de tous types. Pour obtenir des conseils de configuration supplémentaires, consultez l'[architecture de référence de sécurité AWS](#).

IAM Identity Center fournit un portail utilisateur sur lequel vos utilisateurs peuvent trouver et accéder aux rôles qui leur sont assignés Compte AWS, aux applications cloud et aux applications personnalisées en un seul 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 des rôles AWS gérés spécifiques afin de AWS Marketplace déléguer la gestion des AWS Marketplace abonnements au sein de votre AWS organisation.

Par exemple, le client A assume un rôle par le biais de la fédération avec la ManagedMarketplace\_ViewOnly politique attachée à ce rôle. Cela signifie que le client A ne peut consulter les abonnements que dans AWS Marketplace. Vous pouvez créer un rôle IAM autorisé à consulter les abonnements et autoriser le client A à [assumer ce rôle](#).

## Création de rôles IAM pour l'accès AWS Marketplace

Vous pouvez utiliser les rôles IAM pour déléguer l'accès à vos AWS ressources.

Pour créer des rôles IAM afin d'attribuer des autorisations AWS Marketplace

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. Dans Ajouter des autorisations, sélectionnez l'une des politiques suivantes :
  - Pour autoriser uniquement l'affichage des abonnements, mais pas leur modification, choisissez AWSMarketplaceRead-only.

- Pour autoriser les autorisations d'abonnement et de désinscription, choisissez `AWSMarketplaceManageSubscriptions`.
  - Pour permettre un contrôle complet de vos abonnements, choisissez `AWSMarketplaceFullAccess`.
5. Choisissez Suivant.
  6. Dans Nom du rôle, entrez le nom du rôle. Par exemple, `MarketplaceReadOnly` ou `MarketplaceFullAccess`. Puis choisissez Create role (Créer un rôle). Pour plus d'informations, consultez la section [Création 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 définies dans les politiques AWS gérées 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, consultez les sections [Gestion des politiques IAM](#) et [Ajout d'autorisations d'identité IAM](#).

## AWS politiques gérées pour AWS Marketplace

Vous pouvez utiliser des politiques AWS gérées pour fournir des AWS Marketplace autorisations de base. 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 politiques AWS Marketplace gérées de base suivantes sont à votre disposition pour contrôler qui dispose de quelles autorisations :

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`



- `AWSMarketplaceFullAccess`

AWS Marketplace fournit également des politiques gérées spécialisées pour des scénarios spécifiques. Pour obtenir la liste complète des politiques gérées par AWS pour AWS Marketplace les acheteurs, ainsi que les descriptions des autorisations qu'ils fournissent, consultez [AWS politiques gérées pour les AWS Marketplace acheteurs](#).

## Autorisations pour travailler avec License Manager

AWS Marketplace s'intègre AWS License Manager pour 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 dans AWS Marketplace, un utilisateur doit être en mesure de répertorier les informations de licence provenant de AWS License Manager.

Pour vous assurer que vos utilisateurs disposent des autorisations nécessaires pour accéder à toutes les données relatives à leurs AWS Marketplace produits et abonnements, ajoutez l'autorisation suivante :

- `license-manager:ListReceivedLicenses`

Pour plus d'informations sur la définition des autorisations, consultez [la section Gestion des politiques IAM](#) dans le Guide de l'utilisateur IAM.

## Ressources supplémentaires

Pour plus d'informations sur la gestion des rôles IAM, consultez la section [Identités IAM \(utilisateurs, groupes d'utilisateurs et rôles\)](#) dans le guide de l'utilisateur IAM.

Pour plus d'informations sur la gestion des autorisations et des politiques IAM, consultez la section [Contrôle de l'accès aux AWS ressources à l'aide de politiques](#) dans le Guide 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, consultez la section [Gestion des identités et des accès dans AWS Data Exchange](#) dans le guide de l'utilisateur d'AWS Data Exchange.

## AWS politiques gérées pour les AWS Marketplace acheteurs

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

Cette section répertorie chacune des politiques utilisées pour gérer l'accès des acheteurs à AWS 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 : AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWS politique gérée : AWSMarketplaceFullAccess](#)
- [AWS politique gérée : AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWS politique gérée : AWSMarketplaceManageSubscriptions](#)
- [AWS politique gérée : AWSMarketplaceProcurementSystemAdminFullAccess](#)
- [AWS politique gérée : AWSMarketplaceRead -only](#)
- [AWS politique gérée : AWSPrivateMarketplaceAdminFullAccess](#)
- [AWS politique gérée : AWSPrivateMarketplaceRequests](#)
- [AWS politique gérée : AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWS politique gérée : AWSVendorInsightsAssessorFullAccess](#)
- [AWS politique gérée : AWSVendorInsightsAssessorReadOnly](#)
- [AWS Marketplace mises à jour des politiques AWS gérées](#)

## AWS politique gérée : AWSMarketplaceDeploymentServiceRolePolicy

Vous ne pouvez pas joindre de `AWSMarketplaceDeploymentServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet d' AWS Marketplace 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.

## AWS politique 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 le AWS 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 de l'autorisation

```
{
  "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/*"
            ]
        }
    }
}

```

AWS politique gérée :

## AWSMarketplaceLicenseManagementServiceRolePolicy

Vous ne pouvez pas vous associer AWSMarketplaceLicenseManagementServiceRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet d' AWS Marketplace 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 de l'autorisation

```
{
```

```
"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": [
      "*"
    ]
  }
]
```

## AWS politique 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 de l'autorisation

```
{
  "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"
      ]
    }
  ]
}

```

AWS politique 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 Marketplace achats électroniques, y compris la liste des comptes de votre organisation. Pour plus d'informations sur les intégrations d'achats électroniques, consultez.

[Intégration AWS Marketplace aux systèmes d'approvisionnement](#)

Détails de l'autorisation

```

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

```



```

    ],
    "Resource": [
        "*"
    ]
  }
]
}

```

## AWS politique 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 sur AWS Marketplace, ainsi que de consulter les ressources Amazon EC2 AWS Identity and Access Management et Amazon SNS du compte.

### Détails de l'autorisation

```

{
  "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"
    ]
}
]
}

```

## AWS politique 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, consultez [the section called "Création de politiques personnalisées pour les administrateurs de marchés privés"](#).

### Détails de l'autorisation

```

{
  "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": "*"
}
]
```

## AWS politique 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 de l'autorisation

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource": "*"
    }
  ]
}
```

## AWS politique gérée : 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 décrire AWS Organizations.

## AWS politique 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 Marketplace Vendor Insights identifie que l'évaluateur est égal à l'acheteur et le fournisseur est égal au vendeur.

### Détails de l'autorisation

```
{
  "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/*"
}
]
}

```

## AWS politique 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 Marketplace Vendor Insights identifie l'évaluateur comme l'acheteur et le vendeur est égal au vendeur aux fins de ce guide.

### Détails de l'autorisation

```

{
    "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/*"
  }
]
}

```

## AWS Marketplace mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées 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
Suppression de l'ancienne AWSMarketplaceImageBuildFullAccess AWS Marketplace politique	AWS Marketplace a abandonné la méthode de livraison Private Image Build, de sorte que la AWSMarketplaceImageBuildFullAccess politique a également été abandonnée.	30 mai 2024
<a href="#">AWSServiceRoleForPrivateMarketplaceAdminPolicy</a> — Ajout d'une politique pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplace a ajouté une nouvelle politique pour soutenir la gestion des ressources du Private Marketplace et les décrire AWS Organizations.	16 février 2024

Modification	Description	Date
<a href="#">AWSPrivateMarketplaceAdminFullAccess</a> – Mise à jour de la politique existante	AWS Marketplace a mis à jour la politique pour soutenir la lecture AWS Organizations des données.	16 février 2024
<a href="#">AWSMarketplaceDeploymentServiceRolePolicy</a> — Ajout d'une politique pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplace a ajouté une nouvelle politique pour prendre en charge la gestion des paramètres liés au déploiement.	29 novembre 2023
<a href="#">AWSMarketplaceRead-uniquement</a> et <a href="#">AWSMarketplaceManageSubscriptions</a> — mises à jour des politiques existantes	AWS Marketplace a mis à jour les politiques existantes pour autoriser l'accès à la page des offres privées.	19 janvier 2023
<a href="#">AWSPrivateMarketplaceAdminFullAccess</a> – Mise à jour de la politique existante	AWS Marketplace a mis à jour la politique relative à la nouvelle fonctionnalité d'autorisation basée sur des balises.	9 décembre 2022
<a href="#">AWSVendorInsightsAssessorReadOnly</a> AWS Marketplace mis à jour <code>AWSVendorInsightsAssessorReadOnly</code>	AWS Marketplace mis <code>AWSVendorInsightsAssessorReadOnly</code> à jour pour ajouter un accès en lecture seule aux rapports d'un rapport AWS Artifact tiers (version préliminaire).	30 novembre 2022



Modification	Description	Date
<a href="#">AWSVendorInsightsAssessorFullAccess</a> AWS Marketplace mis à jour AWSVendorInsightsAssessorFullAccess	AWS Marketplace mis à jour pour ajouter la recherche d'accords et l'accès en lecture seule au rapport AWS Artifact tiers (aperçu).	30 novembre 2022
<a href="#">AWSVendorInsightsAssessorFullAccess</a> et <a href="#">AWSVendorInsightsAssessorReadOnly</a> — Ajout de politiques pour les nouvelles fonctionnalités dans AWS Marketplace	AWS Marketplace politiques ajoutées pour la nouvelle fonctionnalité AWS Marketplace Vendor Insights : AWSVendorInsightsAssessorFullAccess et AWSVendorInsightsAssessorReadOnly	26 juillet 2022
<a href="#">AWSMarketplaceFullAccess</a> et <a href="#">AWSMarketplaceImagereBuildFullAccess</a> — Mises à jour d'une politique existante	AWS Marketplace a supprimé les autorisations qui ne sont plus nécessaires pour améliorer la sécurité.	4 mars 2022
<a href="#">AWSPrivateMarketplaceAdminFullAccess</a> – Mise à jour d'une politique existante	AWS Marketplace a supprimé les autorisations non utilisées dans la <code>AWSPrivateMarketplaceAdminFullAccess</code> politique.	27 août 2021
<a href="#">AWSMarketplaceFullAccess</a> – Mise à jour d'une politique existante	AWS Marketplace a supprimé une <code>ec2:DescribeAccountAttributes</code> autorisation dupliquée de <code>AWSMarketplaceFullAccess</code> la politique.	20 juillet 2021

Modification	Description	Date
AWS Marketplace a commencé à suivre les modifications	AWS Marketplace a commencé à suivre les modifications apportées AWS à ses politiques gérées.	20 avril 2021

## Trouver votre Compte AWS numéro pour le support client

Si vous ou vos utilisateurs avez besoin de nous contacter AWS Support, vous avez besoin de votre Compte AWS numéro.

Pour trouver votre Compte AWS numéro

1. Connectez-vous à l'[AWS Management Console](#) aide de votre nom d'utilisateur.
2. Dans la barre de navigation supérieure, choisissez Support, puis Centre de support.

Votre Compte 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 AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié 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 AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Marketplace Les rôles liés au service sont prédéfinis par AWS Marketplace et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services 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 Marketplace définit 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 organisation AWS License Manager, vous devez accorder AWS Marketplace des autorisations pour chaque compte avec lequel vous souhaitez partager. Pour ce faire, utilisez le `AWSServiceRoleForMarketplaceLicenseManagement` rôle. 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 [AWS Services 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 de rôle liées au service pour AWS Marketplace

AWS Marketplace utilise le rôle lié au service nommé.

`AWSServiceRoleForMarketplaceLicenseManagement` Ce rôle fournit AWS Marketplace des autorisations pour créer et gérer des licences AWS License Manager pour les produits auxquels vous êtes abonné AWS Marketplace.

Le rôle `AWSServiceRoleForMarketplaceLicenseManagement` lié 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 `AWSServiceRoleForMarketplaceLicenseManagementServiceRolePolicy` AWS Marketplace permet 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 Marketplace crée 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 Marketplace la console](#), connectez-vous et choisissez Paramètres.
2. Dans la section AWS Organizations Intégration, 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 interne AWS Organizations. Par conséquent, outre 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 Marketplace la console](#), connectez-vous et choisissez Paramètres.
2. Dans la section AWS Organizations Intégration, 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 licences AWS 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 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 plus d'informations, consultez la section [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

## Supprimer un rôle lié à un service pour AWS Marketplace

Si vous n'avez plus besoin d'utiliser une fonctionnalité 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 AWS Marketplace service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'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 AWS CLI, le ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForMarketplaceLicenseManagementservice`. 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 de rôles liés au service partout 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 AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié 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 vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Marketplace définit 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'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. Cela protège vos AWS Marketplace ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès 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 de rôle liées à un service pour AWS Marketplace

AWS Marketplace utilise le rôle lié au service

nommé `AWSServiceRoleForMarketplacePurchaseOrders`: ce rôle fournit AWS Marketplace les autorisations nécessaires pour associer des numéros de bon de commande à vos AWS Marketplace abonnements dans AWS Billing and Cost Management

Le rôle `AWSServiceRoleForMarketplacePurchaseOrders` lié à un service fait confiance aux services suivants pour assumer le rôle :

- `purchase-orders.marketplace.amazonaws.com`

La politique d'autorisations de rôle nommée `AWSMarketplacePurchaseOrdersServiceRolePolicy` AWS Marketplace permet 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 avec AWS 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 Marketplace console](#), 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 avec AWS 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 `AWSServiceRoleForMarketplacePurchaseOrders` 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 plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le guide de l'utilisateur IAM.

## Supprimer un rôle lié à un service pour AWS Marketplace

Si vous n'avez plus besoin d'utiliser une fonctionnalité 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, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForMarketplacePurchaseOrders` service. 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 de rôles liés au service partout 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 AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié 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 vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Marketplace définit 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'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 Marketplace utilise le rôle lié au service nommé `AWSServiceRoleForMarketplaceDeployment` pour 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 activé AWS Marketplace.

Le rôle `AWSServiceRoleForMarketplaceDeployment` lié à un service fait confiance aux services suivants pour assumer le rôle :

- `deployment.marketplace.amazonaws.com`

Utilisez la politique d'autorisation des rôles nommée

AWSMarketplaceDeploymentServiceRolePolicy pour 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 Marketplace crée 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'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du deployment.marketplace.amazonaws.com service. Pour plus d'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 Marketplace ne 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 plus d'informations, 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 fonctionnalité 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.

**ℹ 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, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForMarketplaceDeploymentService`. 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 AWS Marketplace liés à un service

AWS Marketplace prend en charge l'utilisation de rôles liés au 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 AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié 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 manuellement les autorisations nécessaires. AWS Marketplace définit 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'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 Marketplace utilise le rôle lié au service nommé

AWSServiceRoleForPrivateMarketplaceAdmin pour décrire et mettre à jour les ressources de Private Marketplace et pour décrire. AWS Organizations

Le rôle AWSServiceRoleForPrivateMarketplaceAdmin lié à un service fait confiance aux services suivants pour assumer le rôle :

- `private-marketplace.marketplace.amazonaws.com`

Utilisez la politique d'autorisation de rôle nommée

AWSServiceRoleForPrivateMarketplaceAdminPolicy pour 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 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 au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, 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 fonctionnalité 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, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForPrivateMarketplaceAdminservice`. 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 AWS Marketplace liés à un service

AWS Marketplace prend en charge l'utilisation de rôles liés au 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, voir [the 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, consultez [the section called “AWSPrivateMarketplaceAdminFullAccess”](#). Pour en savoir plus sur les autres politiques à utiliser AWS Marketplace, connectez-vous au AWS Management Console, puis rendez-vous sur la [page des politiques IAM](#). Dans le champ de recherche, entrez **Marketplace** pour trouver toutes les politiques associées à AWS 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 privé AWS 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 Marketplace acheteur.

Pour être informé des mises à jour de cette documentation, vous pouvez vous abonner au flux RSS.

Modification	Description	Date
<a href="#">Options de modification du contrat annuel Amazon Machine Image (AMI) mises à jour</a>	Les acheteurs peuvent désormais modifier leur abonnement pour ajouter ou changer de type d'instance AMI.	30 mai 2024
<a href="#">Suppression de la AWSMarketplaceImageBuildFullAccess politique</a>	AWS Marketplace a abandonné la méthode de livraison Private Image Build, de sorte que la AWSMarketplaceImageBuildFullAccess politique a également été abandonnée.	30 mai 2024
<a href="#">Nouvelles options de démonstration et d'offre privée sur AWS Marketplace</a>	AWS Marketplace prend désormais en charge les options de <a href="#">démonstration</a> et de demande d' <a href="#">offre privée</a> sur les pages détaillées des produits sélectionnés.	1er avril 2024
<a href="#">Politique de AWS Organizations support mise à jour</a>	Politique gérée mise à jour AWSPrivateMarketplaceAdminFullAccess pour autoriser l'accès aux AWS Organizations données en lecture.	16 février 2024

<a href="#"><u>Nouveau rôle lié au service pour les produits dans AWS Marketplace</u></a>	AWS Marketplace fournit 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
<a href="#"><u>Nouvelle expérience de marché privé sur AWS Marketplace</u></a>	AWS Marketplace prend 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
<a href="#"><u>Disponibilité générale pour les contrats futurs en AWS Marketplace</u></a>	La fonctionnalité des contrats à date future pour tous les ISV et partenaires de distribution du SaaS est désormais généralement disponible dans AWS Marketplace. En utilisant des contrats à date future, les clients peuvent réserver à l'avance des offres ou configurer des renouvellements lorsqu'ils ont déjà acheté des produits sur la même liste de produits, tout en réduisant leurs efforts opérationnels.	16 janvier 2024
<a href="#"><u>Support pour la région du Canada Ouest (Calgary)</u></a>	AWS Marketplace prend désormais en charge ce qui suit Région AWS : Canada West (Calgary).	20 décembre 2023

<a href="#"><u>Nouveau rôle lié au service pour les produits dans AWS Marketplace</u></a>	AWS Marketplace fournit désormais un rôle lié au service pour gérer les paramètres liés au déploiement, qui sont stockés sous forme de secrets pour le compte des AWS Secrets Manager acheteurs.	29 novembre 2023
<a href="#"><u>Nouvelle option de déploiement de Quick Launch pour les acheteurs</u></a>	Les acheteurs peuvent désormais réduire le temps, les ressources et les étapes nécessaires à la configuration, au déploiement et au lancement de produits SaaS (Software as a Service) applicables dans AWS Marketplace.	29 novembre 2023
<a href="#"><u>Des calendriers de paiement flexibles sont disponibles pour les offres privées</u></a>	Les calendriers de paiement flexibles (FPS) pour les offres privées sont désormais disponibles pour tous les clients du AWS Marketplace.	17 novembre 2023
<a href="#"><u>Modules complémentaires tiers d'Amazon EKS</u></a>	Les clients peuvent désormais s'abonner à des modules complémentaires tiers depuis la console Amazon EKS sans être redirigés vers AWS Marketplace.	18 octobre 2023
<a href="#"><u>Support pour Amazon EventBridge</u></a>	AWS Marketplace est désormais intégré à Amazon EventBridge, anciennement Amazon CloudWatch Events.	6 septembre 2023



<a href="#">Support à la région d'Israël (Tel Aviv)</a>	AWS Marketplace soutient désormais ce qui suit Région AWS : Israël (Tel Aviv).	1er août 2023
<a href="#">Assistance aux bons de commande pour les contrats annuels AMI</a>	AWS Marketplace prend désormais en charge la fonctionnalité de commande pour les contrats annuels Amazon Machine Image (AMI).	29 juin 2023
<a href="#">Disponibilité des bons de commande dans AWS Billing la console</a>	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 correspondants.	3 février 2023
<a href="#">Support pour la région Asie-Pacifique (Melbourne)</a>	AWS Marketplace prend désormais en charge les Région AWS systèmes suivants : Asie-Pacifique (Melbourne).	24 janvier 2023
<a href="#">Page des politiques mises à jour pour les offres privées</a>	Politiques gérées mises AWSMarketplaceManagementSubscriptions à jour AWSMarketplaceRead-only et autorisation d'accès à la page des offres privées.	19 janvier 2023

<a href="#">Page d'offres privées</a>	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
<a href="#">Notifications par e-mail mises à jour pour les acheteurs</a>	Les acheteurs sont désormais avertis lorsqu'une offre privée est publiée.	22 décembre 2022
<a href="#">Les essais gratuits du SaaS pour les abonnements sont désormais disponibles pour les acheteurs sur AWS Marketplace</a>	Les acheteurs peuvent désormais s'abonner à des essais gratuits pour les produits SaaS par abonnement.	16 décembre 2022
<a href="#">Les acheteurs peuvent accepter une mise à niveau ou un renouvellement d'une offre privée SaaS</a>	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
<a href="#">AWS Marketplace prend en charge l'archivage des expériences des marchés privés</a>	Les acheteurs peuvent désormais archiver et réactiver les expériences des marchés privés dans AWS Marketplace.	12 décembre 2022
<a href="#">Politique mise à jour pour la fonctionnalité d'autorisation AWS Marketplace basée sur des balises</a>	Mise à jour de la AWSPrivateMarketplaceAdminFullAccess politique pour prendre en charge l'autorisation basée sur des balises dans AWS Marketplace.	9 décembre 2022

<a href="#"><u>Ajout d'une nouvelle rubrique fournisseur des informations sur la façon d'annuler votre abonnement</u></a>	Ajout d'informations sur la manière d'annuler votre abonnement aux produits AMI, ML et SaaS dans AWS Marketplace. Nous avons également ajouté des informations sur l'annulation du renouvellement automatique d'un contrat SaaS.	8 décembre 2022
<a href="#"><u>Politiques mises à jour pour les acheteurs dans AWS Marketplace Vendor Insights</u></a>	Politiques gérées mises à jour AWSVendorInsightsAssessorFullAccess et AWSVendorInsightsAssessorReadOnly pour les acheteurs de AWS Marketplace Vendor Insights.	30 novembre 2022
<a href="#"><u>Contrôle de l'accès des acheteurs dans AWS Marketplace Vendor Insights</u></a>	Ajout d'une nouvelle rubrique dans AWS Marketplace Vendor Insights pour décrire les actions et les autorisations disponibles pour les acheteurs .	30 novembre 2022
<a href="#"><u>Support pour la région Asie-Pacifique (Hyderabad)</u></a>	AWS Marketplace prend désormais en charge les systèmes suivants Région AWS : Asie-Pacifique (Hyderabad).	22 novembre 2022
<a href="#"><u>Support pour la région Europe (Espagne)</u></a>	AWS Marketplace prend désormais en charge les éléments suivants Région AWS : Europe (Espagne).	16 novembre 2022

<a href="#"><u>Support pour la région Europe (Zurich)</u></a>	AWS Marketplace prend désormais en charge les éléments suivants Région AWS : Europe (Zurich).	9 novembre 2022
<a href="#"><u>AWS Marketplace mise à niveau du site Web vers IPv6 d'ici décembre 2022</u></a>	Les acheteurs qui utilisent actuellement l'adresse au format IPv4 dans leurs politiques IAM sont invités à mettre à jour leurs politiques IAM vers des adresses au format IPv6 avant le 15 décembre 2022.	29 septembre 2022
<a href="#"><u>AWS Marketplace Autorisations granulaires sur le marché privé</u></a>	Les acheteurs disposent désormais d'autorisations plus précises pour gérer les expériences des marchés privés.	8 septembre 2022
<a href="#"><u>Ajout de deux politiques pour AWS Marketplace Vendor Insights.</u></a>	Ajout de deux politiques <code>AWSVendorInsightsAssessorFullAccess</code> et <code>AWSVendorInsightsAssessorReadOnly</code> pour AWS Marketplace Vendor Insights, d'une fonctionnalité proposant une évaluation des risques logiciels	26 juillet 2022
<a href="#"><u>AWS Marketplace Informations sur les fournisseurs</u></a>	AWS Marketplace Vendor Insights est une fonctionnalité d'évaluation des risques logiciels.	26 juillet 2022

<a href="#"><u>Mise à jour des méthodes de paiement</u></a>	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
<a href="#"><u>Essais gratuits de SaaS pour les contrats</u></a>	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
<a href="#"><u>Des balises de mesure du fournisseur ont été ajoutées pour les produits AMI, Container et SaaS</u></a>	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
<a href="#"><u>Notifications par e-mail ajoutées aux transactions des acheteurs</u></a>	Nouvelle fonctionnalité permettant d'envoyer des notifications par e-mail à l'acheteur pour vérifier les accords conclus AWS Marketplace.	23 mai 2022
<a href="#"><u>L'approbation automatique des produits Free/BYOL pour les clients d'eProcurement est activée</u></a>	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

<a href="#"><u>Modifications de contrat activées pour les acheteurs dans les contrats AMI et Container Product</u></a>	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
<a href="#"><u>Possibilité de suivre l'utilisation des licences</u></a>	Les acheteurs peuvent désormais suivre les indicateurs de licence basés sur l'utilisation pour les produits AMI et SaaS avec AWS License Manager.	28 mars 2022
<a href="#"><u>Mises à jour de la version Helm CLI</u></a>	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
<a href="#"><u>Mises à jour des politiques gérées existantes</u></a>	Les autorisations qui n'étaient plus nécessaires ont été supprimées des politiques suivantes : <code>AWSPMarketplaceFullAccess</code> et <code>AWSPMarketplaceImageBuildFullAccess</code> .	4 mars 2022

[Possibilité pour les acheteurs basés dans la région EMEA d'acheter des produits via Amazon Web Services EMEA SARL](#)

AWS Marketplace les 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 Marketplace prend 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

<a href="#">Documentation ajoutée pour QuickLaunch</a>	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
<a href="#">Tarification contractuelle pour les produits basés sur l'AMI et les produits basés sur des conteneurs</a>	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
<a href="#">Support pour les bons de commande dans les produits SaaS</a>	AWS Marketplace prend en charge l'ajout de numéros de bon de commande aux contrats d'achat de logiciels en tant que service (SaaS).	28 octobre 2021
<a href="#">Support pour l'intégration de SAP Ariba</a>	AWS Marketplace prend en charge l'intégration avec le système d'approvisionnement SAP Ariba.	13 octobre 2021
<a href="#">Support pour les alias d'AMI</a>	AWS Marketplace prend en charge l'utilisation d'alias pour les ID d'AMI qui peuvent être utilisés dans toutes les régions.	8 septembre 2021



<a href="#"><u>Suppression des autorisations non utilisées dans la politique gérée</u></a>	Les autorisations non utilisées de la politique AWSPrivat eMarketplaceAdminFullAccess AWS gérée ont été supprimées.	27 août 2021
<a href="#"><u>Support pour le partage de licences via AWS License Manager</u></a>	Vous pouvez partager les licences des produits que vous achetez avec d'autres comptes de votre AWS organisation.	3 décembre 2020
<a href="#"><u>AWS Marketplace soutient les offres de services professionnels</u></a>	AWS Marketplace prend désormais en charge l'achat de services professionnels.	3 décembre 2020
<a href="#"><u>Support pour la devise préférée</u></a>	Vous pouvez payer vos AWS Marketplace achats dans la devise de votre choix.	27 juillet 2020
<a href="#"><u>Vous pouvez consulter et accepter les mises à niveau et les renouvellements des offres privées</u></a>	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
<a href="#"><u>AWS Marketplace prend en charge les produits de données via AWS Data Exchange</u></a>	Vous pouvez désormais vous abonner aux produits de données AWS Data Exchange dans AWS Marketplace.	13 novembre 2019

---

<a href="#"><u>AWS Marketplace prend en charge les conteneurs payés à l'heure</u></a>	AWS Marketplace prend désormais en charge les conteneurs horaires payants exécutés sur Amazon Elastic Kubernetes Service (Amazon EKS).	25 septembre 2019
<a href="#"><u>Offres privées mises à jour sur AWS Marketplace</u></a>	Mise à jour du contenu pour plus d'informations sur l'acceptation de différents types d'offres privées.	29 mars 2019
<a href="#"><u>Sécurité mise à jour sur AWS Marketplace</u></a>	Informations sur les politiques IAM mises à jour, section restructurée pour plus de lisibilité.	25 mars 2019
<a href="#"><u>Ajout de contenu pour la fonctionnalité de marché privé</u></a>	Ajout de contenu prenant en charge le lancement de Private Marketplace.	27 novembre 2018
<a href="#"><u>Première publication du guide de l'utilisateur pour les acheteurs</u></a>	Publication initiale 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.