



Guida all'acquisto

Marketplace AWS



Marketplace AWS: Guida all'acquisto

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è Marketplace AWS?	1
Struttura del contratto inMarketplace AWS	2
Aggiornamenti EULA	3
Contratti standard perMarketplace AWS	4
UtilizzandoMarketplace AWScome acquirente	5
Software e Servizi su AWS Marketplace	6
Differenze traMarketplace AWSe Amazon DevPay	8
Iniziare come acquirente	9
Acquisto di elementi di	9
Avvio del software	10
Tutorial: acquisto di un prodotto software basato su AMI	10
Fase 1: creazione di unAccount AWS	11
Fase 2: Scelta del software	11
Fase 3: Configurazione del software	12
Fase 4: Avvio del software su Amazon EC2	13
Fase 5: Gestione del software	14
Fase 6: terminazione dell'istanza	15
Ulteriori informazioni	15
Regioni supportate	16
Categorie di prodotto	18
Software dell'infrastruttura	18
DevOps	19
Applicazioni aziendali	20
Machine Learning	21
IoT	22
Servizi professionali	23
Applicazioni desktop	23
Prodotti dati	25
I industries	25
Tipologie di prodotto	26
Prodotti server basati su AMI	26
Modello AWS CloudFormation	27
Elenchi AMI	28
Prodotti AMI con prezzi contrattuali	29

Prodotti AMI abilitati alla misurazione	34
Etichettatura dell'allocazione dei costi nei prodotti AMI	34
Creata di immagini private	37
Utilizzo di alias AMI	50
Prodotti container	51
Modelli di prezzo per i prodotti container a pagamento	52
Panoramica dei container e di Kubernetes	52
Ricerca e abbonamento ai prodotti container	53
Prodotti container con prezzi contrattuali	57
Avvio del software per container	62
Prodotti per l'apprendimento automatico	68
Pacchetto SageMaker modello Amazon	68
Algoritmo Amazon SageMaker	69
Trova, sottoscrivi e distribuisci	70
Prodotti per servizi professionali	73
Acquisto di servizi professionali	73
Prodotti SaaS	74
Modelli tariffari	74
Avvio rapido	77
Prodotti Data	79
Pagamento dei prodotti	80
Ordini di acquisto	81
Utilizzo degli ordini di acquisto per Marketplace AWS le transazioni	81
Utilizzo degli ordini di acquisto con utilizzo generalizzato	82
Risoluzione dei problemi relativi agli ordini	83
Informazioni sui rimborsi	86
Annullare l'abbonamento al prodotto	86
Annullare l'abbonamento SaaS	87
Annullare l'abbonamento al machine learning	87
Annullare l'abbonamento AMI	88
Annulla il rinnovo automatico dell'abbonamento al contratto SaaS	88
Metodi di pagamento	89
Errori di pagamento	89
Valute supportate	89
Cambiare la valuta preferita	90
Aggiornamento delle istruzioni per le rimesse	91

Etichettatura per l'allocazione dei costi	93
Etichette misurate dal fornitore	93
Argomenti correlati	37
Mercati privati	95
Visualizzazione delle pagine dei dettagli del prodotto	96
Abbonamento a un prodotto in un marketplace privato	96
Abbonamento a un prodotto privato in un marketplace privato	96
Richiedere l'aggiunta di un prodotto al tuo marketplace privato	97
Creazione e gestione di un marketplace privato	97
Guida introduttiva a Private Marketplace	97
Gestione del mercato privato	98
Creazione di un'esperienza di marketplace privata	100
Aggiungere prodotti alla tua esperienza di marketplace privato	100
Verifica dei prodotti nella tua esperienza di marketplace privata	101
Personalizzazione della tua esperienza sul marketplace privato	101
Gestire il pubblico	102
Configurazione del tuo marketplace privato	102
Lavorare con prodotti privati	103
Gestione delle richieste degli utenti	103
Archiviazione e riattivazione di un'esperienza di marketplace privata	104
Offerte private	106
Tipi di prodotto idonei per le offerte private	107
Prepararsi ad accettare un'offerta privata	111
Verifica delle tue preferenze AWS Billing and Cost Management	111
Verifica del metodo di pagamento	111
Verifica delle impostazioni fiscali	111
Visualizzazione e sottoscrizione di un'offerta privata	111
Visualizzazione e sottoscrizione a un'offerta privata da un elenco di offerte private	112
Visualizzazione e sottoscrizione di un'offerta privata tramite un link fornito dal venditore	112
Visualizzazione e sottoscrizione di un'offerta privata dalla pagina del prodotto	113
Risoluzione dei problemi relativi alle offerte private	113
Quando faccio clic sull'ID dell'offerta per visualizzare l'offerta privata, ricevo l'errore Page not found (404)	114
Nessuno di questi suggerimenti funziona	114
Pagina delle offerte private in Marketplace AWS	115
Comprendere la pagina delle offerte private	115

Autorizzazioni necessarie per visualizzare la pagina delle offerte private	116
Abbonamento a un'offerta privata SaaS	116
Iscrizione a un'offerta privata AMI	119
Abbonamento a un'offerta privata AMI annuale con un programma di pagamento flessibile .	121
Abbonamento a un'offerta privata AMI annuale senza un programma di pagamento flessibile	122
Modifica o annullamento dell'iscrizione a un'offerta privata	123
Passaggio dai prezzi delle offerte pubbliche a quelli privati	123
Modifica di un contratto SaaS: aggiornamenti e rinnovi	124
Passaggio da un abbonamento SaaS a un contratto SaaS	124
Passaggio da un contratto AMI a un nuovo contratto	125
Passaggio da AMI a cadenza oraria a AMI annuale	125
Passaggio dall'AMI annuale all'AMI ogni ora	125
Lavorare con accordi con date future	126
Creazione di accordi con data futura	127
Utilizzo di uno strumento di pianificazione dei pagamenti flessibile con accordi con date future	127
Modifica dei contratti con data futura	128
Ricezione di notifiche per accordi con date future	128
Condivisione degli abbonamenti in un'organizzazione	129
Prerequisiti per la condivisione delle licenze	129
Visualizzazione delle licenze	130
Condivisione delle licenze	131
Monitoraggio dell'uso della licenza	131
Notifiche	132
Notifiche e-mail	132
EventBridge Notifiche Amazon	132
Marketplace AWS EventBridge Eventi Amazon dell'API Discovery	133
Integrazione del sistema di approvvigionamento	135
Come funziona l'integrazione degli approvvigionamenti	135
Configurazione dell'integrazione del sistema di approvvigionamento	137
Configurazione delle autorizzazioni IAM	138
Configurazione Marketplace AWS per l'integrazione con Coupa	139
Configurazione Marketplace AWS per l'integrazione con SAP Ariba	140
Codici UNSPSC utilizzati da Marketplace AWS	142
Disattivazione dell'integrazione del sistema di approvvigionamento	142

Prove libere	144
Prezzi del software e dell'infrastruttura	144
Prove gratuite per prodotti basati su AMI	144
Prove gratuite per prodotti a base di contenitori	145
Prove libere di prodotti di machine learning	145
Prove gratuite per prodotti SaaS	146
Utilizzo del piano di utilizzo gratuito AWS con AWS Marketplace	147
Aggiungere abbonamenti AWS Marketplace ad AWS Service Catalog	148
Recensioni di prodotti	149
Linee guida	149
Restrizioni	149
Tempi e aspettative	150
Ottenere supporto	151
Marketplace AWS Vendor Insights	152
Iniziare come acquirente	153
Trova prodotti con Marketplace AWS Vendor Insights	153
Richiedi l'accesso ai dati di valutazione iscrivendoti	154
Annulla l'iscrizione ai dati di valutazione	154
Visualizzazione del profilo di sicurezza di un prodotto	155
Marketplace AWSDashboard in Vendor Insights	155
Visualizza il profilo di sicurezza di un prodotto SaaS	156
Comprensione delle categorie di controllo	156
Esportazione di snapshot	212
Esporta un'istantanea	153
.....	154
Controllo dell'accesso	213
Autorizzazioni per gli acquirenti di Marketplace AWS Vendor Insights	214
GetProfileAccessTerms	214
ListEntitledSecurityProfiles	214
ListEntitledSecurityProfileSnapshots	214
GetEntitledSecurityProfileSnapshot	214
Sicurezza attiva Marketplace AWS	215
Informazioni sugli abbonati condivise con i venditori	215
Aggiorna le policy IAM a IPv6	216
Clienti interessati dall'aggiornamento da IPv6 a IPv6	216
Che cos'è IPv6?	216

Aggiornamento di una policy IAM per IPv6	217
Test della rete dopo l'aggiornamento da IPv6 a IPv6	218
Controllo dell'accesso a Marketplace AWS sottoscrizioni	219
Creazione di ruoli IAM per Marketplace AWS accesso	220
Policy gestite da AWS per Marketplace AWS	221
Autorizzazioni per l'utilizzo di License Manager	221
Risorse aggiuntive	222
AWS policy gestite	222
AWS MarketplaceDeploymentServiceRolePolicy	223
AWS MarketplaceFullAccess	223
AWS MarketplaceImageBuildFullAccess	227
AWS MarketplaceLicenseManagementServiceRolePolicy	231
AWS MarketplaceManageSubscriptions	232
AWS MarketplaceProcurementSystemAdminFullAccess	233
AWS MarketplaceRead-solo	233
AWS PrivateMarketplaceAdminFullAccess	235
AWS PrivateMarketplaceRequests	236
AWS Policy gestita: AWS ServiceRoleForPrivateMarketplaceAdminPolicy	237
AWS VendorInsightsAssessorFullAccess	237
AWS VendorInsightsAssessorReadOnly	238
Aggiornamenti di Marketplace AWS alle policy gestite da AWS	239
Individuazione del Account AWS numero per l'assistenza clienti	242
Uso di ruoli collegati ai servizi	242
Ruoli per condividere i diritti	243
Ruoli per gli ordini di acquisto	246
Ruoli per configurare e lanciare Marketplace AWS prodotti	249
Ruoli per configurare Private Marketplace	253
Creazione di un amministratore del marketplace privato	257
Creazione di politiche personalizzate per gli amministratori del marketplace privato	258
Cronologia dei documenti	261
AWS Glossario	272
.....	cclxxiii

Cos'è Marketplace AWS?

Marketplace AWS è un catalogo digitale curato che puoi utilizzare per trovare, acquistare, distribuire e gestire software, dati e servizi di terze parti necessari per creare soluzioni e gestire le tue attività. Marketplace AWS include migliaia di elenchi di software di categorie popolari come sicurezza, networking, archiviazione, apprendimento automatico, IoT, business intelligence, database e DevOps. Marketplace AWS semplifica inoltre le licenze e l'approvvigionamento del software con opzioni di prezzo flessibili e diversi metodi di implementazione. Inoltre, Marketplace AWS include prodotti di dati disponibili da AWS Data Exchange.

Puoi avviare rapidamente software preconfigurato con pochi clic e scegliere soluzioni software nei formati Amazon Machine Images (AMI) e Software as a Service (SaaS), oltre ad altri formati. Inoltre, puoi sfogliare e abbonarti ai prodotti di dati. Le opzioni di prezzo flessibili includono una prova gratuita, una tariffa oraria, mensile, annuale, pluriennale e un modello Bring Your Own License (BYOL). Tutte queste opzioni di prezzo vengono fatturate da un'unica fonte. AWS gestisce la fatturazione e i pagamenti e gli addebiti vengono visualizzati sulla AWS fattura.

Puoi usare Marketplace AWS come acquirente (abbonato) o come venditore (fornitore), o entrambi. Chiunque abbia un Account AWS può usare Marketplace AWS come consumatore e può registrarsi per diventare venditore. Un venditore può essere un fornitore di software indipendente (ISV), un rivenditore a valore aggiunto o un individuo che ha qualcosa da offrire che funzioni AWS prodotti e servizi.

Note

I fornitori di prodotti di dati devono soddisfare i requisiti di idoneità di AWS Data Exchange. Per ulteriori informazioni, consulta [Fornitura di prodotti dati su AWS Data Exchange](#) nella Guida per l'utente di AWS Data Exchange.

Tutti i prodotti software in Marketplace AWS sono stati sottoposti a un processo di cura. Nella pagina del prodotto possono essere presenti una o più offerte relative al prodotto. Quando il venditore invia un prodotto in Marketplace AWS, definiscono il prezzo del prodotto e i termini e le condizioni d'uso. Gli acquirenti accettano i prezzi e i termini e le condizioni stabiliti per l'offerta.

Nel Marketplace AWS, il prodotto può essere utilizzato gratuitamente o può avere un costo associato. L'addebito diventa parte della tua AWS fattura, e dopo aver pagato, Marketplace AWS paga il venditore.

Note

Al momento dell'acquisto da [alcuni venditori non statunitensi](#), potresti anche ricevere una fattura fiscale dal venditore. Per ulteriori informazioni, consulta [Venditori di AWS Marketplaces](#) su [Assistenza fiscale su Amazon Web Service](#).

I prodotti possono assumere molte forme. Ad esempio, un prodotto può essere offerto come Amazon Machine Image (AMI) istanziata utilizzando Account AWS. Il prodotto può anche essere configurato per l'uso AWS CloudFormation modelli per la consegna al consumatore. Il prodotto potrebbe anche essere costituito da offerte SaaS (Software as a Service) di un ISV o un ACL Web, un insieme di regole o condizioni per AWS WAF.

È possibile acquistare prodotti software al prezzo di listino utilizzando il contratto di licenza standard per l'utente finale (EULA) dell'ISV o tramite un'offerta privata con prezzi personalizzati ed EULA. È inoltre possibile acquistare prodotti con un [contratto standard](#) con limiti di tempo o utilizzo specificati.

Dopo aver sottoscritto gli abbonamenti ai prodotti, puoi utilizzare AWS Service Catalog per copiare il prodotto e gestire le modalità di accesso e utilizzo del prodotto nell'organizzazione. Per ulteriori informazioni, vedere [Aggiungere Marketplace AWS Prodotti al tuo portafoglio](#) nel AWS Service Catalog Guida per l'amministratore.

Struttura del contratto in Marketplace AWS

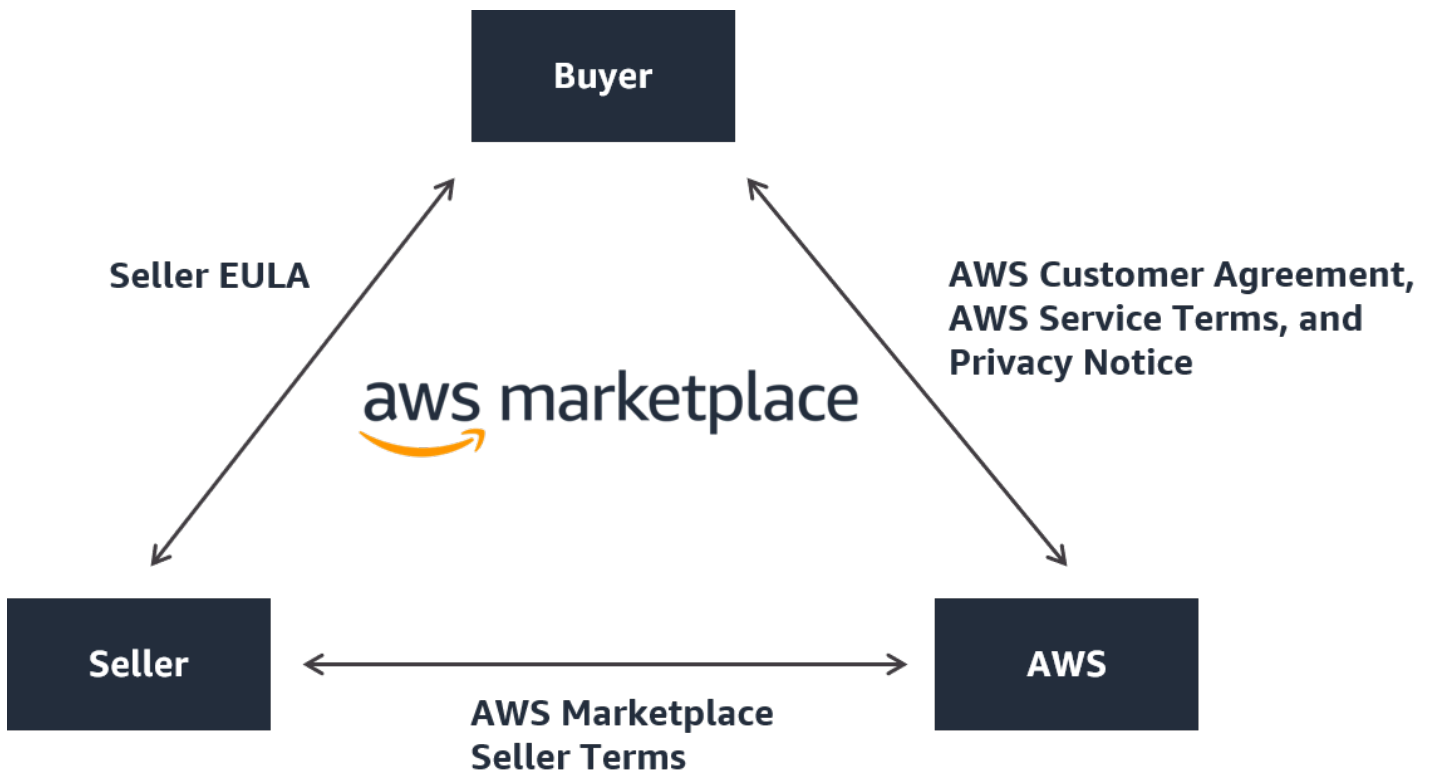
Utilizzo del software, dei servizi e dei prodotti di dati venduti Marketplace AWS è regolato da accordi tra acquirenti e venditori. AWS non è parte di questi accordi.

In qualità di acquirente, il tuo utilizzo di Marketplace AWS è regolato dal [Termini di servizio AWS](#), il [Contratto con il cliente AWS](#) e il [Informativa sulla privacy](#).

I contratti di vendita includono quanto segue:

- L'EULA del venditore si trova nella pagina di elenco dei prodotti relativa alle offerte di software pubbliche su Marketplace AWS. Molti venditori utilizzano [Contratto standard per Marketplace AWS \(SCMP\)](#) come EULA predefinito. Possono inoltre utilizzare l'SCMP come base per le negoziazioni nelle offerte private e utilizzare il modello di modifica per modificare l'SCMP. Le offerte private possono includere anche condizioni contrattuali personalizzate negoziate tra le parti.
- [Marketplace AWS Termini del venditore](#) regolano l'attività del venditore in Marketplace AWS.

Il grafico seguente mostra la struttura del contratto per Marketplace AWS.



Aggiornamenti EULA

I venditori hanno la possibilità di aggiornare l'EULA per ciascuno dei loro prodotti Software as a Service (SaaS). L'impatto di questo aggiornamento sull'EULA dipende dal tipo di offerta e dal modello di prezzo.

La tabella seguente fornisce informazioni su quando il nuovo EULA entrerà in vigore per i prodotti SaaS.

Tipo di offerta	Modello tariffario	Una volta aggiornato, l'EULA ha effetto
Pubblica	Utilizzo	Annullo l'abbonamento e ti iscrivi nuovamente.
Pubblica	Contratto	Il contratto attuale scade e si rinnova in un nuovo contratto di offerta pubblica.

Tipo di offerta	Modello tariffario	Una volta aggiornato, l'EULA ha effetto
Pubblica	Contratto con consumo	Il contratto attuale scade e si rinnova in un nuovo contratto di offerta pubblica.
Privata	Utilizzo	La tua attuale offerta privata scade e si rinnova automaticamente in un nuovo contratto di offerta pubblica. I rinnovi dell'offerta privata dipendono dall'offerta privata specifica.
Privata	Contratto	La tua attuale offerta privata scade e ti iscrivi nuovamente e all'offerta pubblica o a una nuova offerta privata. I rinnovi dell'offerta privata dipendono dall'offerta privata specifica.
Privata	Contratto con consumo	La tua attuale offerta privata scade e ti iscrivi nuovamente e all'offerta pubblica o a una nuova offerta privata. I rinnovi dell'offerta privata dipendono dall'offerta privata specifica.

Contratti standard perMarketplace AWS

Mentre ti prepari all'acquisto di un prodotto, consulta l'EULA o il contratto standardizzato associato. Molti venditori offrono lo stesso contratto standardizzato nelle loro inserzioni, il [Contratto standard perMarketplace AWS\(SCMP\)](#). Marketplace AWS ha sviluppato l'SCMP in collaborazione con le comunità di acquirenti e venditori per regolamentare l'utilizzo e definire gli obblighi di acquirenti e venditori per le soluzioni digitali. Esempi di soluzioni digitali includono software per server, software as a service (SaaS) e algoritmi di intelligenza artificiale e apprendimento automatico (AI/ML).

Invece di esaminare gli EULA personalizzati per ogni acquisto, è sufficiente rivedere l'SCMP una sola volta. La [termini del contratto](#) sono uguali per tutti i prodotti che utilizzano SCMP.

I venditori possono anche utilizzare i seguenti addendum con SCMP:

- [Addendum sulla sicurezza avanzata](#)— Supporta transazioni con elevati requisiti di sicurezza dei dati.
- [Addendum HIPAA Business Associate](#)— Supporta le transazioni ai sensi dei requisiti di conformità all'Health Insurance Portability and Accountability Act del 1996 (HIPAA).

Per trovare elenchi di prodotti che offrono contratti standardizzati, utilizza il Contratto standard filtra durante la ricerca di prodotti. Per le offerte private, chiedi al venditore se può sostituire l'EULA con l'SCMP e applicare le modifiche concordate, se necessario, per supportare i requisiti specifici della transazione.

Per ulteriori informazioni, consulta [Contratti standardizzati in Marketplace AWS](#).

Utilizzando Marketplace AWS come acquirente

Come acquirente, vai a [Marketplace AWS](#) per cercare, filtrare e accedere a un prodotto che funziona su Amazon Web Services.

Quando scegli un prodotto software, verrai indirizzato alla pagina del prodotto. La pagina contiene informazioni sul prodotto, sui prezzi, sull'utilizzo, sull'assistenza e sulle recensioni dei prodotti. Per abbonarsi al prodotto software, accedi al Account AWS e vengono indirizzati a una pagina di abbonamento che contiene l'EULA, i termini e le condizioni d'uso e tutte le opzioni disponibili per personalizzare l'abbonamento.

Marketplace AWS gli acquisti effettuati dai tuoi account con sede in Europa, Medio Oriente e Africa (esclusi Turchia e Sud Africa) presso venditori idonei all'area EMEA sono facilitati da Amazon Web Services EMEA SARL.

Per i clienti di alcuni paesi, Amazon Web Services EMEA SARL addebita l'imposta sul valore aggiunto (IVA) locale sul Marketplace AWS acquisti. Per ulteriori informazioni sulle imposte, consulta la [Pagina di assistenza fiscale per gli acquirenti di AWS Marketplace](#).

Per ulteriori informazioni su Amazon Web Services EMEA SARL, consulta la [Domande frequenti su Amazon Web Services EMEA SARL](#).

I clienti che effettuano transazioni con venditori idonei all'area EMEA ricevono una fattura da Amazon Web Services EMEA SARL. Tutte le altre transazioni continuano ad essere eseguite AWS Inc. Per ulteriori informazioni, vedere [Pagamento dei prodotti](#).

Dopo l'elaborazione dell'abbonamento, puoi configurare le opzioni di adempimento, le versioni del software e Regioni AWS dove desideri utilizzare il prodotto, quindi avviare il prodotto software. Puoi anche trovare o lanciare i tuoi prodotti visitando [Il tuo software Marketplaces](#) sul Marketplace AWS sito web, dal tuo Marketplace AWS o la console Amazon Elastic Compute Cloud (Amazon EC2) o tramite il Service Catalog.

Per ulteriori informazioni sulle categorie di prodotti disponibili utilizzando Marketplace AWS, vedi [Categorie di prodotto](#).

Per ulteriori informazioni sui metodi di consegna dei prodotti software in Marketplace AWS, vedi:

- [Prodotti server basati su AMI](#)
- [Prodotti container](#)
- [Prodotti per l'apprendimento automatico](#)
- [Prodotti per servizi professionali](#)
- [Prodotti SaaS](#)
- Prodotti di dati: vedi [Cos'è AWS Data Exchange?](#) nel Guida per l'utente di AWS Data Exchange

Software e Servizi su AWS Marketplace

Marketplace AWS include diverse categorie software, database, server applicazioni, server applicazioni, monitoraggio e gestione dei contenuti, nonché software di business intelligence. software di business Intelligence È possibile selezionare software commerciali da venditori noti, nonché molte offerte open source ampiamente utilizzate. Quando trovi i prodotti che desideri, puoi acquistare e distribuire il software sulla tua istanza Amazon EC2 con 1-Click. È possibile utilizzare anche AWS CloudFormation per implementare una topologia del prodotto.

Qualsiasi AWS il cliente può fare acquisti su Marketplace AWS. I prezzi del software e i prezzi stimati dell'infrastruttura sono visualizzati sul sito web. È possibile acquistare immediatamente la maggior parte dei software, utilizzando gli strumenti di pagamento già registrati con AWS. I costi del software sono riportati sulla stessa fattura mensile di AWS canoni infrastrutturali.

Note

- Molti prodotti aziendali sono disponibili nella Marketplace AWS, inclusi sia software as a service (SaaS) che prodotti basati su server. I prodotti basati su server potrebbero richiedere conoscenze tecniche o supporto IT per la configurazione e la manutenzione.
- Le informazioni e le esercitazioni in [Tutorial: Nozioni di base sulle istanze Amazon EC2 Linux](#) può aiutarti a imparare le basi di Amazon EC2.
- Se si prevede di avviare topologie complesse di Marketplace AWS prodotti tramite AWS CloudFormation, [Nozioni di base su AWS CloudFormation](#) può rivelarsi utile su AWS CloudFormation Nozioni di base

Marketplace AWS include le categorie seguenti di software:

- Software per l'infrastruttura
- Strumenti per sviluppatori
- Software aziendale
- Machine learning
- IoT
- Servizi professionali
- Applicazioni desktop
- Prodotti dati

Per ulteriori informazioni, consulta la pagina [Categorie di prodotto](#) .

Ogni categoria di software principale contiene sottocategorie più specifiche. Ad esempio, la categoria Software Infrastruttura contiene sottocategorie quali Sviluppo applicazioni, Database e memorizzazione nella cache e Sistemi operativi. Il software è disponibile come uno dei sette diversi tipi di prodotto, tra cui Amazon Machine Images (AMI) e Software as a Service (SaaS). Per ulteriori informazioni sui diversi tipi di software, consulta [Tipologie di prodotto](#).

Per aiutarti nella scelta del software di cui hai bisogno, Marketplace AWS fornisce le informazioni che seguono:

- Informazioni sul venditore

- Versione software
- Tipo di software (AMI o SaaS) e informazioni sull'AMI, se applicabile
- Valutazione dell'acquirente
- Prezzo
- Informazioni sui prodotti

Differenze tra Marketplace AWS e Amazon DevPay

Esistono differenze sostanziali tra Marketplace AWS e Amazon DevPay. Entrambi aiutano i clienti ad acquistare software che gira su AWS, ma Marketplace AWS offre un'esperienza più completa rispetto ad Amazon DevPay. Per gli acquirenti di software, le differenze principali sono le seguenti:

- Marketplace AWS offre un'esperienza di acquisto più simile ad Amazon.com, semplificando la scoperta del software disponibile.
- Marketplace AWS i prodotti funzionano con altre AWS funzionalità come il cloud privato virtuale (VPC) e può essere eseguito su istanze riservate e istanze Spot di Amazon Elastic Compute Cloud (Amazon EC2), oltre alle istanze on demand.
- Marketplace AWS supporta software supportato da Amazon Elastic Block Store (Amazon EBS) e Amazon DevPay non la include.

Inoltre, i venditori di software traggono vantaggio dalla divulgazione del marketing e dalla facilità di scoperta di Marketplace AWS.

Iniziare come acquirente

I seguenti argomenti descrivono il processo iniziale di Marketplace AWS acquisto di prodotti software.

Argomenti

- [Acquisto di elementi di](#)
- [Avvio del software](#)
- [Tutorial: acquisto di un prodotto software basato su AMI](#)
- [Ulteriori informazioni](#)

Per informazioni su come iniziare a utilizzare i prodotti dati, consulta [Iscrizione ai prodotti dati su AWS Data Exchange](#) nella Guida per l'utente di AWS Data Exchange.

Acquisto di elementi di

Nello stato Marketplace AWS, l'acquisto di un prodotto significa che hai accettato i termini del prodotto come mostrato nella pagina delle offerte del prodotto. Ciò include i termini di prezzo e il contratto di licenza con l'utente finale (EULA) del venditore e che l'utente accetta di utilizzare tale prodotto in conformità con il [Accordo con i clienti AWS](#). Riceverai una notifica e-mail all'indirizzo e-mail associato al Account AWS per le offerte accettate in Marketplace AWS.

Se il prodotto ha un canone mensile o è acquistato con un contratto di abbonamento, ti verrà addebitato il costo al momento dell'abbonamento. L'abbonamento è ripartito proporzionalmente in base al tempo rimanente nel mese. Non vengono addebitati altri addebiti finché non esegui una delle seguenti operazioni:

- Avvia un'istanza Amazon Elastic Compute Cloud (Amazon EC2) con Amazon Machine Image (AMI).
- Implementare il prodotto utilizzando un AWS CloudFormation template.
- Registra il prodotto sul sito web del venditore.

Se il prodotto ha un'opzione di abbonamento annuale, ti verrà addebitato l'intero canone annuale al momento dell'abbonamento. Questo addebito copre la base di utilizzo del prodotto, con il rinnovo dell'abbonamento dovuto nell'anniversario della data di abbonamento originale. Se non si rinnova alla

fine del periodo di abbonamento annuale, l'abbonamento si converte in un abbonamento orario alla tariffa oraria corrente.

Per ulteriori informazioni sugli abbonamenti ai prodotti dati, consulta [Iscrizione a prodotti di dati su AWS Data Exchange](#) nella AWS Data Exchange.

Avvio del software

Dopo l'acquisto del software, puoi avviare le Amazon Machine Images (AMI) utilizzando la Avvio a 1 clic visualizzazione in Marketplace AWS. Puoi avviarlo anche utilizzando altri Amazon Web Services (AWS) strumenti di gestione, tra cui AWS Management Console la console Amazon Elastic Compute Cloud (Amazon EC2), le API Amazon EC2 o la AWS CloudFormation Console -.

Con la Avvio a 1 clic, è possibile rivedere, modificare e quindi avviare rapidamente una singola istanza del software con le impostazioni consigliate dal venditore del software. La Lancio con la console EC2view fornisce un modo semplice per trovare il numero di identificazione dell'AMI e altre informazioni pertinenti necessarie per avviare l'AMI utilizzando il AWS Management Console, API Amazon EC2 o altri strumenti di gestione. La Lancio con la console EC2view offre anche più opzioni di configurazione rispetto all'avvio dal AWS Management Console, ad esempio l'assegnazione di tag a un'istanza.

Per Marketplace AWS prodotti con topologie complesse, Lancio personalizzato view fornisce un Avviare con CloudFormation Console opzione che carica il prodotto nel AWS CloudFormation console con l'apposito AWS CloudFormation Template. È quindi possibile seguire i passaggi indicati nella AWS CloudFormation procedura guidata della console per creare il cluster di AMI e associati AWS risorse per quel prodotto.

Tutorial: acquisto di un prodotto software basato su AMI

Il tutorial seguente descrive come acquistare un prodotto Amazon Machine Image () con Marketplace AWS.

Fasi

- [Fase 1: creazione di un Account AWS](#)
- [Fase 2: Scelta del software](#)
- [Fase 3: Configurazione del software](#)
- [Fase 4: Avvio del software su Amazon EC2](#)
- [Fase 5: Gestione del software](#)

- [Fase 6: terminazione dell'istanza](#)

Fase 1: creazione di unAccount AWS

Puoi navigare nelMarketplace AWS sito Web (<https://aws.amazon.com/marketplace>) senza effettuare l'accesso al tuoAccount AWS. Tuttavia, devi effettuare l'accesso per abbonarti o lanciare prodotti.

È necessario aver effettuato l'accesso allaAccount AWS per accedere allaMarketplace AWS console. Per informazioni su come creare unAccount AWS, vedere [Creazione di unAccount AWS](#) nella GuidaAWS Account Management di riferimento.

Fase 2: Scelta del software

Per scegliere il tuo software

1. Accedere al [Marketplace AWSsito Web](#).

Note

Puoi acquistare, abbonarti e lanciare nuove istanze dalMarketplace AWS sito Web pubblico, all'indirizzo <https://aws.amazon.com/marketplace>AWS Management Console, o tramiteMarketplace AWS <https://console.aws.amazon.com/marketplace/home#/subscriptions>.

Le esperienze nelle due sedi sono simili. Questa procedura utilizza ilMarketplace AWS sito Web ma rileva eventuali differenze importanti nell'utilizzo della console.

2. Il riquadro Acquista tutte le categorie contiene l'elenco delle categorie tra cui puoi scegliere. Puoi anche scegliere il software presente nel riquadro centrale. Per questo tutorial, nel riquadro Acquista tutte le categorie, scegli Gestione dei contenuti.
3. Dall'elenco Content Management, scegli WordPressCertified by Bitnami e Automattic.
4. Nella pagina dei dettagli del prodotto, consulta le informazioni sul prodotto. La pagina dei dettagli del prodotto include informazioni aggiuntive come:
 - Valutazione dell'acquirente
 - Offerta di Support
 - Caratteristiche
 - Descrizione dettagliata del prodotto

- Dettagli sui prezzi per i tipi di istanze in ciascuna di esse Regione AWS (per le AMI)
 - Ulteriori risorse per iniziare
5. Scegliere Continue to Subscribe (Continua la sottoscrizione).
 6. Se non l'hai ancora fatto, ti verrà chiesto di accedere alla Marketplace AWS. Se disponi già di un Account AWS, puoi utilizzare quell'account per accedere. Se non si dispone di un Account AWS, consulta [Fase 1: creazione di un Account AWS](#).
 7. Leggi i termini dell'offerta di Bitnami, quindi scegli Accetta contratto per accettare l'offerta di abbonamento.
 8. Il completamento dell'azione di iscrizione potrebbe richiedere alcuni istanti. In tal caso, riceverai un messaggio di posta elettronica sui termini dell'abbonamento e potrai continuare. Scegli Continua con la configurazione per configurare e avviare il software.

L'abbonamento a un prodotto significa che hai accettato i termini del prodotto. Se il prodotto ha un canone mensile, al momento dell'abbonamento ti viene addebitato il canone, che viene ripartito proporzionalmente in base al tempo rimanente nel mese. Non verranno addebitati altri costi fino al lancio di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) con AMI API scelta.

Note

In qualità di abbonato a un prodotto, il tuo account riceverà messaggi e-mail quando viene pubblicata una nuova versione del software a cui sei abbonato.

Fase 3: Configurazione del software

Poiché abbiamo scelto il software come AMI, il passaggio successivo consiste nella configurazione del software, inclusa la selezione del metodo di consegna, della versione e Regione AWS in cui si desidera utilizzare il software.

Per configurare il software

1. Nella pagina Configura questo software, seleziona Amazon Machine Image (AMI) a 64 bit (x86) come metodo di consegna.
2. Scegli l'ultima versione disponibile per la versione del software.
3. Scegli la regione in cui desideri lanciare il prodotto, ad esempio Stati Uniti orientali (Virginia settentrionale).

Note

Man mano che apporti modifiche alla configurazione, potresti notare che l'ID Ami nella parte inferiore dello schermo si aggiorna. Il formato dell'ID è `ami.<identifier>`, ad esempio, `ami-123example456`. Ogni versione di ogni prodotto in ogni regione ha un AMI diverso. Questo ID AMI consente di specificare l'AMI corretto da utilizzare all'avvio del prodotto. L'alias Ami è un ID simile che è più facile da usare nell'automazione. Per ulteriori informazioni sull'alias (per ulteriori informazioni sull'alias, consulta la pagina relativa all'alias [Utilizzo di alias AMI](#)).

4. Seleziona Continua all'avvio.

Fase 4: Avvio del software su Amazon EC2

Prima di avviare l'istanza Amazon EC2, devi decidere se avviare l'istanza con 1 clic o se utilizzare la console Amazon EC2. L'avvio con 1 clic consente l'avvio rapido con le opzioni predefinite consigliate, come i gruppi di sicurezza e i tipi di istanza. Con il lancio di 1-Click, puoi anche vedere la tua fattura mensile stimata. Se preferisci altre opzioni, come l'avvio in un Amazon Virtual Private Cloud (Amazon VPC), dovresti avviare l'avvio utilizzando la console Amazon EC2. Le seguenti procedure illustrano la sottoscrizione al prodotto e il lancio di un'istanza EC2 utilizzando 1-Click Launch o la console Amazon EC2.

Avvio su Amazon EC2 con avvio in 1 clic

Per eseguire il lancio su Amazon EC2 utilizzando l'avvio in 1 clic

1. Nella pagina **Avvia questo software**, scegli **Avvia dal sito Web** nel menu a discesa **Scegli azione** e rivedi le impostazioni predefinite. Se desideri modificarne uno, procedi nel seguente modo:
 - Nell'elenco a discesa **Tipo di istanza EC2**, scegli un tipo di istanza.
 - Negli elenchi a discesa **Impostazioni VPC** e **Impostazioni subnet**, seleziona le impostazioni di rete che desideri utilizzare.
 - Nelle **Impostazioni del gruppo di sicurezza**, scegli un gruppo di sicurezza esistente o scegli **Crea nuovo** in base alle impostazioni del venditore per accettare le impostazioni predefinite. Per ulteriori informazioni sui gruppi di sicurezza, consulta [Gruppi di sicurezza Amazon EC2 per istanze Linux](#) nella Guida per l'utente di Amazon EC2 per istanze Linux.

- Espandi Key Pair e scegli una key pair esistente, se ne hai una. Se non si dispone di una key pair, viene richiesto di crearla. Per ulteriori informazioni sulle coppie di chiavi Amazon EC2, consulta [Coppie di chiavi Amazon EC2](#).
2. Se le impostazioni ti soddisfano, scegli Avvia.

La tua nuova istanza viene avviata con il software WordPressCertified by Bitnami e Automatic in esecuzione su di essa. Da qui, puoi visualizzare i dettagli dell'istanza, creare un'altra istanza o visualizzare tutte le istanze del tuo software.

Lancio su Amazon EC2 utilizzando la console Launch with EC2

Per eseguire il lancio su Amazon EC2 utilizzando la console Launch with EC2

1. Nella pagina Avvia su EC2, scegli la vista Avvia con la console EC2, quindi seleziona una versione AMI dall'elenco Seleziona una versione.
2. Consulta le impostazioni del firewall, le istruzioni di installazione e le note di rilascio, quindi scegli Avvia con la console EC2.
3. Nella console EC2, avvia l'AMI utilizzando la Request Instance Wizard. Segui le istruzioni in [Nozioni di base sulle istanze Linux di Amazon EC2](#) per navigare nella procedura guidata.

Fase 5: Gestione del software

In qualsiasi momento, puoi gestire gli abbonamenti softwareMarketplace AWS utilizzando la pagina Gestisci abbonamenti della [Marketplace AWSconsole](#).

Per gestire il tuo software

1. Vai alla [Marketplace AWSconsole](#) e scegli Gestisci abbonamenti.
2. Nella pagina Gestisci abbonamenti:
 - Visualizzazione dello stato dell'istanza per prodotto
 - Visualizzazione degli addebiti mensili correnti
 - Esegui una nuova istanza
 - Visualizza i profili dei venditori per la tua istanza
 - Gestisci le tue istanze
 - Collegati direttamente alla tua istanza Amazon EC2 per configurare il tuo software

Fase 6: terminazione dell'istanza

Se decidi che l'istanza non è più necessaria, puoi decidere che l'istanza non è più necessaria.

Note

Non puoi riavviare un'istanza interrotta. Puoi tuttavia avviare istanze aggiuntive della stessa (AMI).

Per terminare l'istanza

1. Vai alla [Marketplace AWSconsole](#) e scegli Gestisci abbonamenti.
2. Nella pagina Gestisci abbonamenti, scegli l'abbonamento software di cui desideri terminare un'istanza e seleziona Gestisci.
3. Nella pagina di sottoscrizione specifica, scegli Visualizza istanze dall'elenco a discesa Azioni.
4. Seleziona la regione in cui si trova l'istanza che desideri terminare. La console Amazon EC2 viene aperta e vengono visualizzate le istanze in quella regione in una nuova scheda. Se necessario, puoi tornare a questa scheda per visualizzare l'ID dell'istanza per la chiusura dell'istanza.
5. Nella console Amazon EC2, scegli l'ID dell'istanza per aprire la pagina dei dettagli dell'istanza.
6. Dall'elenco a discesa Stato dell'istanza, scegli Termina istanza.
7. Quando viene richiesta la conferma, seleziona Terminate (Interrompi).

Per il completamento della terminazione sono necessari alcuni minuti.

Ulteriori informazioni

Per ulteriori informazioni sulle categorie e sui tipi di prodotti, consulta [Categorie di prodotto](#) e [Tipologie di prodotto](#).

Per ulteriori informazioni su Amazon EC2, consulta la documentazione del servizio in [Amazon Elastic Cloud Documentation](#).

Per ulteriori informazioniAWS, consulta <https://aws.amazon.com/>.

Regioni AWS supportato in Marketplace AWS

Per quanto riguarda i prodotti software, il venditore sceglie in quali Regioni AWS tipi di istanza rendere disponibile il software. Consigliamo di rendere disponibili i prodotti in tutte le regioni disponibili e su tutti i tipi di istanza che abbiano senso. Il Marketplace AWS sito Web è disponibile in tutto il mondo e supporta le seguenti regioni:

- Nord America
 - Stati Uniti orientali (Ohio)
 - Stati Uniti orientali (Virginia settentrionale)
 - Stati Uniti occidentali (California settentrionale)
 - Stati Uniti occidentali (Oregon)
 - AWS GovCloud (Stati Uniti orientali)
 - AWS GovCloud (Stati Uniti occidentali)
 - Canada (Centrale)
 - Canada occidentale (Calgary)

- Africa
 - Africa (Città del Capo)

- Sud America
 - Sud America (San Paolo)

- EMEA
 - Europa (Francoforte)
 - Europa (Irlanda)
 - Europa (Londra)
 - Europa (Milano)
 - Europa (Parigi)
 - Europa (Spagna)
 - Europa (Stoccolma)
 - Europa (Zurigo)

- APAC
 - Asia Pacifico (Hong Kong)
 - Asia Pacific (Hyderabad)
 - Asia Pacifico (Giacarta)
 - Asia Pacifico (Melbourne)
 - Asia Pacifico (Mumbai)
 - Asia Pacific (Osaka)
 - Asia Pacific (Seul)
 - Asia Pacifico (Singapore)
 - Asia Pacifico (Sydney)
 - Asia Pacifico (Tokyo)

- Medio Oriente
 - Israele (Tel Aviv)
 - Medio Oriente (Bahrein)
 - Medio Oriente (Emirati Arabi Uniti)

Per ulteriori informazioni sulle regioni supportate per i prodotti di dati, consulta gli [endpoint e le quote di AWS Data Exchange](#) nella Guida AWSgenerale.

Categorie di prodotto

La [Marketplace AWS](#) il sito web è organizzato in categorie principali, con sottocategorie sotto ciascuna. È possibile cercare e filtrare in base alle categorie e alle sottocategorie che vengono aggiunti.

Argomenti

- [Software dell'infrastruttura](#)
- [DevOps](#)
- [Applicazioni aziendali](#)
- [Machine Learning](#)
- [IoT](#)
- [Servizi professionali](#)
- [Applicazioni desktop](#)
- [Prodotti dati](#)
- [I industries](#)

Software dell'infrastruttura

I prodotti di questa categoria forniscono soluzioni relative all'infrastruttura.

Backup e ripristino

Prodotti utilizzati per soluzioni di storage e backup.

Data Analytics

Prodotti utilizzati per l'analisi dei dati.

High Performance Computing

Prodotti di elaborazione ad alte prestazioni.

Migrazione

Prodotti utilizzati per progetti di migrazione.

infrastruttura di rete

Prodotti utilizzati per creare soluzioni di rete.

Sistemi operativi

Sistemi operativi Linux e Windows confezionati.

Sicurezza

Prodotti di sicurezza per la tua infrastruttura.

Storage

Applicazioni incentrate sui ruoli professionali coinvolti nello storage.

DevOps

I prodotti di questa categoria forniscono strumenti incentrati su sviluppatori e team di sviluppatori.

Gestione del ciclo di vita

Prodotti utilizzati per Agile SDLM.

Sviluppo delle applicazioni

Prodotti utilizzati per lo sviluppo di applicazioni.

Server applicazioni

Server utilizzati per lo sviluppo di applicazioni

Stack dell'applicazione

Stack utilizzati per lo sviluppo di applicazioni

Integrazione continua e distribuzione continua

Prodotti utilizzati per CI/CD.

Infrastruttura come codice

Prodotti utilizzati per l'infrastruttura.

Monitoraggio dei problemi e dei bug

Prodotti utilizzati dai team di sviluppatori per tracciare e gestire i bug del software.

Monitoraggio

Prodotti utilizzati per il monitoraggio del software operativo.

Log Analysis

Prodotti utilizzati per la registrazione e l'analisi dei log.

Controllo del codice sorgente

Strumenti utilizzati per gestire e mantenere il controllo del codice sorgente.

Test

Prodotti utilizzati per il test automatico di prodotti software.

Applicazioni aziendali

I prodotti di questa categoria ti aiutano a gestire la tua attività.

Blockchain

Prodotti utilizzati per la blockchain.

Collaborazione e produttività

Prodotti utilizzati per consentire la collaborazione nella tua azienda.

Centro di contatto

Prodotti utilizzati per abilitare i Contact Center nella tua organizzazione.

Gestione dei contenuti

Prodotti incentrati sulla gestione dei contenuti.

CRM

Strumenti dedicati alla gestione delle relazioni con i clienti.

eCommerce

Prodotti che forniscono soluzioni di eCommerce.

eLearning

Prodotti che forniscono soluzioni di eLearning.

Risorse umane

Prodotti utilizzati per abilitare le risorse umane nella tua organizzazione.

Gestione aziendale IT

Prodotti utilizzati per abilitare la gestione aziendale IT nella tua organizzazione.

Business Intelligence

Prodotti utilizzati per abilitare la business intelligence nella tua organizzazione.

Gestione del progetto

Strumenti per la gestione dei progetti.

Machine Learning

I prodotti di questa categoria forniscono algoritmi di apprendimento automatico e pacchetti di modelli compatibili con Amazon SageMaker.

Soluzioni ML

Soluzioni di machine learning.

Servizi di etichettatura dei dati

Prodotti che forniscono funzionalità di etichettatura dei dati.

Computer Vision

Prodotti che consentono funzionalità di visione artificiale.

Elaborazione del linguaggio naturale

Prodotti che consentono la capacità di elaborazione del linguaggio naturale.

Riconoscimento vocale

Prodotti che abilitano la funzionalità di riconoscimento vocale.

Text (Testo)

Prodotti che consentono la capacità di apprendimento del testo. Gli esempi includono classificazione, clustering, modifica/elaborazione, incorporamento, generazione, grammatica/analisi, identificazione, nomi e riconoscimento di entità, analisi del sentiment, riepilogo, text-to-speech traduzione.

Image

Prodotti che consentono funzionalità di analisi delle immagini. Gli esempi includono 3D, didascalie, classificazione, modifica/elaborazione, incorporamento/estrazione di feature, generazione, grammatica/analisi, riconoscimento della grafia, uomo/volti, rilevamento di oggetti, segmentazione/etichettatura pixel e testo/OCR.

Video

Prodotti che consentono funzionalità di analisi video. Gli esempi includono classificazione, rilevamento di oggetti, modifica/elaborazione, rilevamento di anomalie, identificazione degli altoparlanti, movimento, reidentificazione, riepilogo, testo/didascale e tracciamento.

Audio

Prodotti che consentono funzionalità di analisi audio. Gli esempi includono l'identificazione degli altoparlanti, speech-to-text, classificazione, identificazione delle canzoni e segmentazione.

Struttura del

Prodotti che consentono funzionalità di analisi strutturata. Gli esempi includono classificazione, clustering, riduzione della dimensionalità, modelli di fattorizzazione, ingegneria delle caratteristiche, classificazione, regressione e previsione di serie temporali.

IoT

Prodotti utilizzati per creare soluzioni correlate all'IoT.

Analisi

Prodotti analitici per soluzioni IoT.

Applicazioni

Prodotti applicativi per lo spazio delle soluzioni IoT.

Connettività dispositivi

Prodotti utilizzati per gestire la connettività dei dispositivi.

Gestione dispositivi

Prodotti utilizzati per gestire i dispositivi.

Sicurezza dei dispositivi

Prodotti utilizzati per gestire la sicurezza dei tuoi dispositivi IoT.

Industrial IoT

Prodotti incentrati sulla fornitura di soluzioni IoT legate all'industria.

Smart Home &

Prodotti utilizzati per abilitare soluzioni smart home e smart city.

Servizi professionali

I prodotti di questa categoria forniscono servizi di consulenza relativi a Marketplace AWS Prodotti .

Valutazione

Valutazione del tuo attuale ambiente operativo per trovare le soluzioni giuste per la tua organizzazione.

Implementazione

Assistenza per la configurazione, la configurazione e l'implementazione di software di terze parti.

Managed Services

End-to-end gestione dell'ambiente per tuo conto.

Premium Support

Accesso alla guida e all'assistenza di esperti, progettati per le tue esigenze.

Training

Workshop, programmi e strumenti didattici personalizzati forniti da esperti per aiutare i tuoi dipendenti ad apprendere le migliori pratiche.

Applicazioni desktop

I prodotti di questa categoria forniscono soluzioni relative all'infrastruttura.

Applicazioni desktop

Applicazioni e utility desktop per la produttività generale e l'abilitazione di ruoli lavorativi specifici.

AP e fatturazione

Applicazioni utilizzate per ruoli lavorativi incentrati sulla contabilità fornitori e sulla fatturazione.

Applicazione e Web

Applicazioni generiche e per ambienti web.

Sviluppo

Applicazioni utilizzate per lo sviluppo.

Business Intelligence

Applicazioni utilizzate da ruoli professionali incentrati sulla gestione della business intelligence.

CAD e CAM

Applicazioni utilizzate da ruoli professionali incentrate sulla progettazione e produzione assistita da computer.

GIS e mapping

Applicazioni utilizzate da ruoli professionali incentrati su GIS e mappatura.

Illustrazione e design

Candidature per ruoli lavorativi incentrate sull'illustrazione e sul design.

Media e codifica

Applicazione utilizzata per ruoli lavorativi coinvolti nei media e nella codifica.

Produttività e collaborazione

Applicazioni incentrate sull'abilitazione della produttività e sull'abilitazione della collaborazione.

Gestione del progetto

Candidatura per ruoli lavorativi di project manager.

Sicurezza/archiviazione/archiviazione

Applicazioni incentrate sui ruoli professionali coinvolti nella sicurezza, nello storage e nell'archiviazione dei dati.

Utilità

Applicazioni incentrate sull'utilità per vari ruoli lavorativi.

Prodotti dati

I prodotti di questa categoria sono insiemi di dati basati su file. Per ulteriori informazioni, consulta la [Guida dell'utente di AWS Data Exchange](#).

I industries

Istruzione e ricerca

Prodotti volti a fornire soluzioni di istruzione e ricerca.

Servizi finanziari

Prodotti che abilitano i servizi finanziari nella tua organizzazione.

Sanità e scienze della vita

Prodotti utilizzati nei settori sanitario e delle scienze della vita.

Media e intrattenimento

Prodotti e soluzioni relativi ai media.

Industrial

Prodotti e soluzioni legati al settore.

Energy

Prodotti e soluzioni legati all'energia.

Tipologie di prodotto

Marketplace AWS include i più diffusi software open source e commerciali, oltre a prodotti di dati gratuiti e a pagamento. Questi prodotti sono disponibili in diversi modi: come singole Amazon Machine Images (AMI), come cluster di AMI distribuiti tramite un AWS CloudFormation modello, come software as a service (SaaS), come servizi professionali e come prodotti dati AWS Data Exchange.

Per ulteriori dettagli su questi tipi di prodotti, consulta i seguenti argomenti:

- [Prodotti server basati su AMI](#) (compresi prodotti AMI e immagini private)
- [Prodotti container](#)
- [Prodotti per l'apprendimento automatico](#)
- [Prodotti per servizi professionali](#)
- [Prodotti SaaS](#)
- [Prodotti Data](#)

Prodotti server basati su AMI

Un'Amazon Machine Image (AMI) è un'immagine di un server, che include un sistema operativo e spesso software aggiuntivo, che viene eseguito su AWS.

Il software elencato in Marketplace AWS è disponibile solo per l'esecuzione su Amazon Elastic Compute Cloud (Amazon EC2). Non è disponibile per il download.

Su Marketplace AWS, puoi cercare AMI (con suggerimenti di ricerca), visualizzare le recensioni dei prodotti inviate da altri clienti, sottoscrivere e lanciare AMI e gestire i tuoi abbonamenti.

Tutti i Marketplace AWS la qualità dei prodotti è stata verificata e preconfigurata per la funzionalità di avvio con 1 clic su Amazon Web Services (AWS) infrastruttura.

Sia gli elenchi di prodotti AMI che quelli del software as a service (SaaS) provengono da venditori affidabili. I prodotti AMI vengono utilizzati all'interno del cliente Account AWS. Mantieni un maggiore controllo sulla configurazione del software e sui server che eseguono il software, ma hai anche responsabilità aggiuntive per quanto riguarda la configurazione e la manutenzione dei server.

Il Marketplace AWS il catalogo contiene una selezione curata di software open source e commerciali di noti venditori. Molti prodotti su Marketplace AWS può essere acquistato a ore.

Il catalogo AMI è una risorsa comunitaria in cui persone e team di sviluppo possono elencare e scambiare software o progetti in fase di sviluppo, senza dover passare attraverso controlli approfonditi. Le inserzioni nel catalogo AMI della community possono provenire o meno da venditori noti e in genere non sono state sottoposte a ulteriori indagini.

Un Marketplace AWS il prodotto contiene un'AMI per ciascuna Regione AWS in cui il prodotto è disponibile. Queste AMI sono identiche ad eccezione della loro ubicazione. Inoltre, quando i venditori aggiornano il prodotto con le patch e gli aggiornamenti più recenti, possono aggiungere un altro set di AMI al prodotto.

Alcuni Marketplace AWS i prodotti possono avviare più istanze di un'AMI perché vengono distribuiti come cluster utilizzando AWS CloudFormation modelli. Questo gruppo di istanze, insieme a ulteriori AWS servizi di infrastruttura configurati da CloudFormation modello, agiscono come un'unica implementazione del prodotto.

Modello AWS CloudFormation

Important

Marketplace AWS interromperà il metodo di consegna per più prodotti Amazon Machine Image (AMI) utilizzando AWS CloudFormation modelli nell'agosto 2024. Altri Marketplace AWS prodotti che utilizzano CloudFormation, ad esempio una singola AMI con CloudFormation, non ne risentirà.

Fino ad agosto 2024, gli abbonati esistenti possono lanciare nuove istanze dei loro molteplici prodotti AMI utilizzando CloudFormation modelli da Marketplace AWS. Dopo l'interruzione, non saranno in grado di avviare nuove istanze. Tutte le istanze esistenti precedentemente lanciate e in esecuzione in Amazon Elastic Compute Cloud (Amazon EC2) non subiranno alcun impatto e continueranno a funzionare.

In caso di domande, contatta [AWS Support](#).

AWS CloudFormation è un servizio che ti aiuta a modellare e configurare le risorse AWS così da poter dedicare meno tempo alla gestione di tali risorse e concentrarsi invece sulle applicazioni eseguite in AWS. Un CloudFormation il modello descrive i vari AWS le risorse che desideri, come le istanze di Amazon Elastic Compute Cloud (Amazon EC2) o le istanze di database Amazon Relational Database Service (Amazon RDS). CloudFormation si occupa del provisioning e della configurazione di tali risorse per te. Per ulteriori informazioni, vedere [Guida introduttiva ad AWS CloudFormation](#).

Usando AWS CloudFormation modelli

I venditori di software possono offrire CloudFormation modelli per definire una topologia di implementazione preferita composta da più istanze AMI e altro AWS risorse. Se un CloudFormation modello è disponibile per un prodotto, verrà elencato come opzione di distribuzione nella pagina di elenco dei prodotti.

Puoi utilizzare un'AMI per distribuire una singola istanza Amazon EC2. Puoi usare un CloudFormation modello per distribuire più istanze di un'AMI che fungono da cluster, insieme a AWS risorse come Amazon RDS, Amazon Simple Storage Service (Amazon S3) o qualsiasi altro AWS servizio: come soluzione unica.

Argomenti

- [Abbonamenti AMI in Marketplace AWS](#)
- [Prodotti AMI con prezzi contrattuali](#)
- [Prodotti AMI abilitati alla misurazione](#)
- [Etichettatura dell'allocazione dei costi nei prodotti AMI](#)
- [Creata di immagini private](#)
- [Utilizzo di alias AMI](#)

Abbonamenti AMI in Marketplace AWS

Nel Marketplace AWS, alcuni prodotti software basati su Amazon Machine Image (AMI) offrono un modello di prezzo di abbonamento annuale. Con questo modello di prezzo, effettui un pagamento anticipato una tantum e non paghi alcuna tariffa oraria per i prossimi 12 mesi. Puoi applicare un abbonamento annuale a un prodotto Marketplace AWS software a un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Note

Per AMI con tariffa oraria con tariffa annuale, l'abbonamento annuale copre solo i tipi di istanze specificati al momento dell'acquisto. Ad esempio, t3.medium. L'avvio di qualsiasi altro tipo di istanza comporterà la tariffa oraria per quel tipo di istanza in base all'abbonamento attivo. Non puoi modificare il tipo di istanza di un abbonamento annuale dopo l'acquisto.

Puoi anche continuare a lanciare ed eseguire prodotti Marketplace AWS software utilizzando prezzi orari. I costi per l'utilizzo di Amazon EC2 e di altri servizi offerti da Amazon AWS sono separati e si aggiungono a quelli pagati per l'acquisto di prodotti Marketplace AWS software.

Se modifichi il tipo di istanza Amazon EC2 per l'utilizzo orario, la tua infrastruttura Amazon EC2 verrà fatturata in base al piano di risparmio firmato. Tuttavia, il modulo di licenza AMI Marketplace AWS passerà automaticamente alla tariffa oraria.

Se un prodotto orario AMI non supporta i prezzi annuali, l'acquirente non può acquistare un abbonamento annuale. Se un prodotto orario AMI supporta i prezzi annuali, l'acquirente può accedere alla pagina del prodotto Marketplace AWS e acquistare contratti annuali. Ogni contratto annuale consente all'acquirente di eseguire un'istanza senza che venga fatturata la tariffa oraria. I contratti variano in base al tipo di istanza.

Prodotti AMI con prezzi contrattuali

Alcuni venditori offrono prodotti software pubblici basati su Amazon Machine Image (AMI) con un modello di prezzo a contratto. In questo modello, accetti di effettuare un pagamento anticipato una tantum per quantità discrete di licenze per accedere al prodotto software per una durata a tua scelta. Ti verrà addebitato, in anticipo, tramite il tuo Account AWS. Ad esempio, è possibile acquistare 10 licenze di accesso utente e 5 licenze amministrative per un anno. Puoi scegliere di rinnovare automaticamente le licenze.

Inoltre, alcune aziende offrono prodotti software privati basati su AMI con un modello di prezzo contrattuale. Un'offerta privata ha in genere una durata fissa che non è possibile modificare.

Puoi acquistare un contratto di prodotto software basato su AMI utilizzando la pagina dei dettagli del prodotto su AWS Marketplace. Se questa opzione è disponibile, AMI con prezzi contrattuali viene visualizzato per Delivery Method (Metodo di consegna) nella pagina prodotto. Quando effettui l'acquisto, verrai indirizzato al sito Web del prodotto per la configurazione e la configurazione dell'account. Le spese di utilizzo verranno quindi visualizzate sul tuo normale Account AWS report di fatturazione.

Abbonamento a un prodotto AMI con offerta pubblica di prezzi contrattuali

Per sottoscrivere un'offerta pubblica prodotto basato su AMI con un modello di prezzo contrattuale

1. Accesso Marketplace AWS e trovare un prodotto software basato su container con un modello di prezzo contrattuale.
2. Sul Procur (Certificato creato) Informazioni sui prezzi.

Puoi visualizzare ilUnitàe la tariffa per ogni durata (in mesi).

3. ScegliereContinuare ad abbonarsiper avviare l'abbonamento.

Per salvare questo prodotto senza sottoscrivere un abbonamento, scegliSalva nell'elenco.

4. Creare un accordo esaminando le informazioni sui prezzi e configurando i termini per il prodotto software.
 - a. Scegli la durata del contratto:1 month,12 mesi,24 mesi, oppure36 mesi
 - b. UnderImpostazioni rinnovo, scegliere se rinnovare automaticamente il contratto.
 - c. UnderOpzioni del contratto, scegli una quantità per ogni unità.

Il prezzo totale del contratto è visualizzato sottoDettagli prezzi.

5. Dopo aver effettuato le selezioni, scegliereCreate CONTRACT.

LaPrezzo totale del contrattoè a carico del tuoAccount AWS. Una licenza è generata inAWS License Manager.

Note

Potrebbero volerci fino a 10 minuti affinché la sottoscrizioni si elabori e la generazione di una licenza nelAWS License Managerconto per il prodotto software.

Abbonamento a un prodotto AMI con offerta privata a prezzi contrattuali

Per sottoscrivere un'offerta privata prodotto basato su AMI con un modello di prezzo contrattuale

1. AccessoMarketplace AWScon il tuo account Acquirente.
2. Visualizza l'offerta privata.
3. SulProcur(Certificato creato)Informazioni sui prezzi.

Puoi visualizzare ilUnitàe la tariffa per ogni durata (in mesi).

4. ScegliereContinuare ad abbonarsiper avviare l'abbonamento.
5. Creare un accordo esaminando le informazioni sui prezzi e configurando i termini per il prodotto software.

La durata del contratto è già stabilita dal Venditore e non può essere modificata.

6. UnderOpzioni del contratto, scegli una quantità per ogni unità.
7. Visualizza il prezzo totale del contratto sottoDettagli prezzi.

Puoi anche visualizzare l'offerta al pubblico scegliendo Visualizzazione offerta sotto Altre offerte disponibili.

8. Dopo aver effettuato le selezioni, scegliere Create CONTRACT.

Note

Potrebbero volerci fino a 10 minuti affinché la sottoscrizione si elabori e la generazione di una licenza nel AWS License Manager conto per il prodotto software.

Accesso al software

Per accedere al prodotto software basato su AMI

1. Sul Marketplace AWS console, vai su Visualizzazione dell'abbonamento e visualizzare la licenza per il prodotto software.
2. Sul Procur (Certificato creato)
 - a. Scegliere Gestione Licenze per visualizzare, concedere l'accesso e monitorare l'utilizzo delle autorizzazioni in AWS License Manager.
 - b. Scegli Continue to Configuration (Passa alla configurazione).
3. Sul Avvio di pagina, rivedi la tua configurazione e scegli come vuoi avviare il software sotto Scegli Action.
4. Sul Scegli il tipo di istanza., scegliere un'istanza Amazon Elastic Compute Cloud (Amazon EC2), quindi scegliere Successivo: Configura i dettagli dell'istanza.
5. Sul Configura i dettagli dell'istanza (Certificato creato) Ruolo IAM, scegli uno esistente AWS Identity and Access Management (IAM) ruolo dal tuo Account AWS.

Se non hai già un ruolo IAM, scegli Creazione di un nuovo ruolo IAM manualmente link e segui le istruzioni.

Note

Quando acquisti un prodotto con prezzi contrattuali, viene creata una licenza da Marketplace AWS sul Account AWS che il software può verificare utilizzando l'API di License Manager. Avrai bisogno di un ruolo IAM per avviare un'istanza del prodotto basato su AMI.

Le seguenti autorizzazioni IAM sono richieste nella politica 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. Dopo aver configurato i dettagli dell'istanza, scegliere **Rivedi** e **avvia**.
7. Sul **Rivedi** l'avvio dell'istanza selezionare una key pair esistente o crearne una nuova, quindi scegliere **Avvio**.

La **Avvio** delle istanze **Viene visualizzata** la finestra di avanzamento

8. Dopo aver avviato l'istanza, vai al dashboard di EC2 e in **Istanze**, consulta che il **Stato** istanza **display** **Correre**.

Visualizzazione di una licenza generata

Per visualizzare una licenza generata

1. Accesso AWS License Manager con il Account AWS.
2. Under License concesse, visualizzare tutte le licenze concesse.
3. Cerca le licenze immettendo lo SKU, il destinatario o lo stato del prodotto nella Cercabar.
4. Seleziona License ID e visualizza il Dettagli licenza.
5. Puoi visualizzare il Approvatore (AWS/Marketplace) e il Diritti (le unità che la licenza concede il diritto di utilizzare, accedere o utilizzare un'applicazione o una risorsa).

Modifica di un contratto esistente

Se hanno già un impegno iniziale per un prodotto AMI, Marketplace AWS gli acquirenti possono modificare alcuni aspetti di un contratto. Un contratto AMI è supportato da offerte basate su condizioni contrattuali rispetto alle offerte FCP (Flexible Consumption Pricing) orarie o annuali. Questa caratteristica è disponibile solo per le applicazioni integrate con AWS License Manager. Gli acquirenti possono acquistare licenze aggiuntive nell'ambito del diritto alla stessa offerta nel contratto in corso. Tuttavia, gli acquirenti non possono ridurre il numero di diritti acquistati nel contratto. Gli acquirenti possono anche annullare il rinnovo automatico dell'abbonamento se l'opzione è abilitata dal venditore.

Note

Un'offerta di contratto FPS (Flexible Payment Schedule) non può essere modificata. Non ci sono modifiche di diritto disponibili per l'acquirente per un contratto acquistato FPS. Un diritto è un diritto di utilizzare, accedere o utilizzare un'applicazione o una risorsa. Le offerte FPS non sono modificabili.

Gestione delle sottoscrizioni

1. Sul Marketplace AWS console, vai su Visualizzazione dell'abbonamento e visualizzare la licenza per il prodotto software.
2. Sul Procur (Seleziona) Gestione Licenza.
3. Dall'elenco, seleziona Visualizzazione dei termini.

4. Nella Opzioni del contratto, aumenta i tuoi diritti usando le frecce. Non è possibile ridurre il numero di diritti al di sotto dei diritti acquistati.
5. I dettagli del contratto e il prezzo totale vengono visualizzati nella Dettagli prezzo sezione.

Per annullare il rinnovo automatico dell'abbonamento

1. Sul Marketplace AWS console, vai su Visualizzazione dell'abbonamento e visualizzare la licenza per il prodotto software.
2. Sul Procur (Seleziona) Gestione Licenza.
3. Sul Subscription pagina, individua il Impostazioni rinnovo sezione.
4. Assicurati di aver compreso i termini e le condizioni con la cancellazione.
5. Selezionare la casella di controllo per annullare il rinnovo automatico.

Prodotti AMI abilitati alla misurazione

Alcuni prodotti elencati su Marketplace AWS sono fatturati in base all'utilizzo misurato dall'applicazione software. Esempi di dimensioni di utilizzo a consumo includono l'utilizzo dei dati, l'utilizzo di host/ agente o l'utilizzo della larghezza di banda. Questi prodotti richiedono una configurazione aggiuntiva per funzionare correttamente. Un ruolo IAM con l'autorizzazione all'utilizzo del contatore deve essere associato al tuo Marketplace AWS Amazon Elastic Compute Cloud (Amazon EC2) al momento del lancio. Per ulteriori informazioni sui ruoli IAM per Amazon EC2, consultare [Ruoli IAM per Amazon EC2](#).

Etichettatura dell'allocazione dei costi nei prodotti AMI

Marketplace AWS supporta l'allocazione dei costi per l'allocazione dei costi per i prodotti software basati su Amazon Machine Image (Amazon Machine Image). I tag di istanza di Amazon Elastic Compute Cloud (Amazon EC2) nuovi ed esistenti vengono utilizzati da Amazon Elastic Compute Cloud (Amazon Marketplace AWS EC2). Puoi utilizzare i tag di allocazione dei costi attivati per identificare e monitorare l'utilizzo delle AMI tramite AWS Cost Explorer i report su AWS costi e utilizzo, AWS i budget o altri strumenti di analisi della spesa nel cloud.

Il fornitore che ha fornito l'AMI può anche registrare altri tag personalizzati nella misurazione dei prodotti basati su AMI, in base alle informazioni specifiche del prodotto. Per ulteriori dettagli, consulta [Etichettatura per l'allocazione dei costi](#).

Puoi utilizzare i tag per organizzare le tue risorse e tenere traccia dei costi di AWS a livello dettagliato. Una volta attivati, AWS i tag per l'allocazione dei costi vengono utilizzati da per organizzare i costi delle risorse nel report di allocazione dei costi AWS.

La tag per l'allocazione dei costi viene utilizzata da per organizzare i costi a partire dal momento in cui i tag per l'allocazione dei costi vengono Billing and Cost Management. Solo Account AWS i proprietari, i proprietari degli account di AWS Organizations gestione e gli utenti con le autorizzazioni appropriate possono accedere alla console di Billing and Cost Management di un account. Indipendentemente dal fatto che utilizzi l'etichettatura per l'allocazione dei costi, l'importo della fatturazione non cambia. L'utilizzo di tag di allocazione dei costi non ha alcun impatto sulla funzionalità dei prodotti software basati su AMI.

Tracciamento dei tag di allocazione dei costi per un'AMI su più istanze

Ogni istanza Amazon EC2 lanciata per un abbonamento Marketplace AWS AMI ha una riga corrispondente sull'utilizzo del Marketplace AWS software nel rapporto AWS Costi e utilizzo. Marketplace AWS L'utilizzo rifletterà sempre i tag specifici applicati all'istanza Amazon EC2 corrispondente. Ciò consente di distinguere i costi di Marketplace AWS utilizzo in base ai diversi valori di tag assegnati, a livello di istanza.

Puoi anche sommare i costi di utilizzo basati sui tag in modo che corrispondano al costo di utilizzo del software AMI riportato nella fattura con il Cost Explorer o il rapporto AWS Costi e utilizzo.

Individuazione di budget con istanze etichettate a costi allocati

Se disponi già di budget attivi filtrati in base ai tag di allocazione dei costi su diverse istanze Amazon EC2 nella console di Billing and Cost Management, potrebbe essere difficile trovarli tutti. Il seguente script Python restituisce un elenco di budget che contengono istanze Amazon EC2 Marketplace AWS a partire da quella corrente Regione AWS.

Puoi utilizzare questo script per conoscere il potenziale impatto sul tuo budget e dove potrebbero verificarsi superamenti a causa di questa modifica. Tieni presente che l'importo fatturato non cambia, ma le allocazioni dei costi verranno riflesse in modo più accurato, il che può influire sui budget.

```
#!/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()
```

Output di esempio

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

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

Argomenti correlati

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Utilizzo dei tag di allocazione dei costi](#) nella Guida perAWS Billing l'utente.
- [Attivazione dei tag di allocazione dei costi generati da AWS](#) nella Guida per l'AWS Billingutente.
- [Tagging delle risorse di Amazon EC2](#) nella Guida per l'utente di Amazon EC2 per istanze Linux.

Creata di immagini private

Important

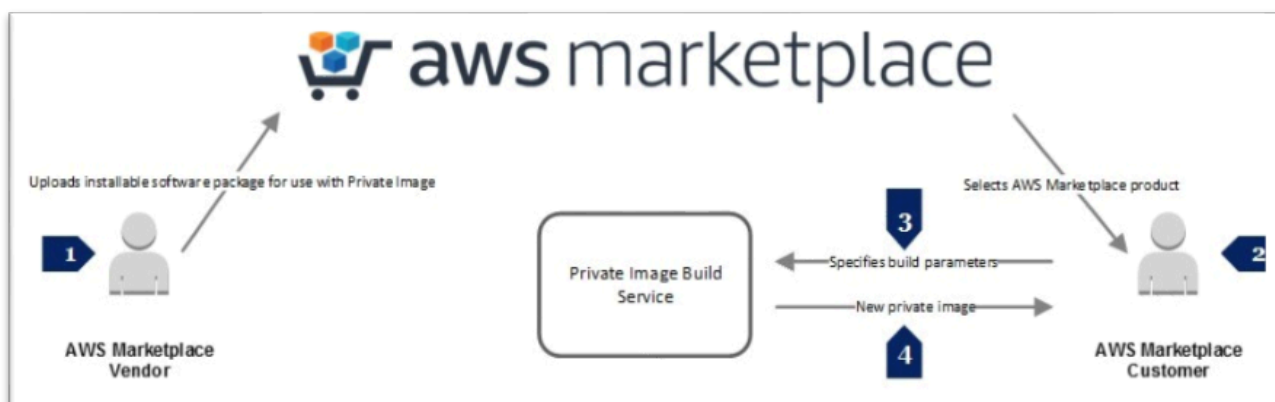
Marketplace AWSinterromperà il metodo di consegna Private Image Build nell'aprile 2024. Fino ad aprile 2024, gli attuali abbonati a Private Image Build possono creare nuove AMI (Amazon Machine Images) dorate o aggiornare le proprie AMI dorate con il software fornito

nel metodo di distribuzione Private Image Build. Dopo l'interruzione, non saranno in grado di creare o aggiornare le proprie AMI con il software Private Image Build. Le AMI esistenti create in precedenza con Private Image Build non sono interessate. Ciò significa che le AMI create con Private Image Build possono continuare a essere fatturate e lanciate utilizzando Amazon Elastic Compute Cloud (Amazon EC2) e le istanze attive continueranno a funzionare come oggi.

Inoltre, il software precedentemente disponibile solo come Private Image Build è ora disponibile tramite l'opzione di adempimento AMI autonoma, che non verrà interrotta. L'AMI standalone può ancora essere utilizzato con l'abbonamento Private Image Build esistente dopo l'interruzione di Private Image Build. In caso di domande, contatta [AWS Support](#).

Marketplace AWS Private Image Build ti consente di acquistare prodotti software installabili Marketplace AWS e quindi installarli su un'immagine gold o un'AMI a tua scelta tra le immagini disponibili nel tuo account AWS. Ai fini di questo contenuto, un'immagine dorata è un'immagine server che include un sistema operativo (OS) di base con modifiche applicate in modo che ogni server avviato da quell'immagine aderisca agli standard IT definiti dall'utente. Scegli il software da Marketplace AWS installare e l'AMI di base per la build. Quindi usi l'AWS Image Build Service per creare e distribuire una nuova AMI come immagine privata disponibile solo per il tuo account AWS.

Questo servizio ti aiuta a soddisfare meglio i requisiti interni di sicurezza, conformità e gestione consentendoti di eseguire Marketplace AWS i prodotti su un sistema operativo di base che soddisfi gli standard IT.



I venditori che partecipano a Marketplace AWS Private Image Build creano versioni installabili del loro prodotto per piattaforme di sistema operativo, sistemi operativi e versioni del sistema operativo specifici. Quando un venditore invia una serie di pacchetti software per il proprio

prodotto, Marketplace AWS Image Build Service installa e scansiona il prodotto sul sistema operativo specificato prima di pubblicarlo Marketplace AWS. Quando acquisti un prodotto abilitato per Marketplace AWS Private Image Build, puoi scegliere un'AMI esistente su cui creare una nuova immagine privata. Dopo aver utilizzato l'Marketplace AWS Image Build Service per creare una nuova immagine, questa diventa disponibile nella tua console Amazon EC2 come immagine di tua proprietà. È possibile creare un'immagine utilizzando il Marketplace AWS sito Web oppure utilizzare l'API Marketplace AWS Image Build Service.

È previsto un costo per il software e i Servizi AWS infrastruttura da utilizzare per completare il processo di creazione, che può richiedere da 1 a 2 ore a seconda del prodotto. Tuttavia, non sono previsti costi aggiuntivi per l'utilizzo delle funzioni private Marketplace AWS definite dall'utente per la creazione di funzioni private. Una volta creata l'immagine, non dovrai sostenere costi per l'utilizzo del prodotto o AWS delle risorse finché non utilizzi il prodotto.

Marketplace AWS Private Image Build utilizza [AWS Identity and Access Management](#) (IAM) per creare ruoli e policy IAM che concedono autorizzazioni limitate agli utenti finali per creare e visualizzare immagini private. Il completamento dei passaggi prerequisiti richiede privilegi di livello amministrativo.

Completamento dei passaggi prerequisiti

Important

Marketplace AWS interromperà il metodo di consegna di Private Image Build nell'aprile 2024. Il metodo di consegna è disponibile solo per gli abbonati esistenti fino alla sua sospensione. Per ulteriori informazioni, consulta [Creazione di immagini private](#).

I passaggi prerequisiti descritti qui richiedono autorizzazioni di configurazione a livello amministrativo AWS Identity and Access Management (IAM) in modo da poter concedere la possibilità di creare immagini private ad altri utenti. Dopo aver creato le policy e i ruoli IAM, puoi collegarli agli account di gruppo (o utente) in modo che gli utenti associati possano creare immagini private.

IAM è un servizio Web che aiuta a controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Si creano [identità](#) (utenti, gruppi e ruoli) e si aggiungono gli utenti ai gruppi in modo da poter gestire i gruppi anziché i singoli utenti. Un ruolo IAM è simile a un utente, in quanto è un'identità con policy di autorizzazione che determinano ciò che l'identità può e non può fare in AWS. Tuttavia, a un ruolo non sono associate credenziali (password o chiavi di accesso). Invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque ne

abbia bisogno. Un utente può assumere un ruolo per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

La parte di [gestione degli accessi](#) di IAM ti aiuta a definire cosa può fare un utente o un'altra entità in un account, spesso denominata autorizzazione. Le autorizzazioni vengono concesse tramite politiche. Una policy è un'entità in AWS che, quando viene collegata a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale, ad esempio un utente, effettua una richiesta. Le autorizzazioni nella policy determinano l'approvazione o il rifiuto della richiesta. Le policy vengono archiviate in AWS come documenti JSON collegati ai principali come policy basate sulle identità o collegati alle risorse come policy basate sulle risorse. Puoi concedere le autorizzazioni definendo i [criteri di autorizzazione](#) e assegnando i criteri a un gruppo.

Le [policy basate su identità sono policy](#) di autorizzazione che è possibile collegare a un principale (o identità), ad esempio un utente, un ruolo o un gruppo. Le policy basate sulle risorse sono documenti di policy JSON che colleghi a una risorsa, come ad esempio un bucket Amazon Simple Storage Service (Amazon S3). Le policy basate su identità controllano quali operazioni l'identità può eseguire, su quali risorse e in quali condizioni. Le policy basate sull'identità possono essere classificate in politiche gestite, politiche AWS gestite dai clienti e politiche in linea.

Le policy basate su risorse controllano quali operazioni uno specifico principale può eseguire, su quale risorsa e in quali condizioni. Le policy basate risorse sono policy inline. Non esistono policy gestite basate su risorse. Sebbene le identità IAM siano tecnicamente AWS risorse, non è possibile collegare una policy basata sulle risorse a un'identità IAM. È necessario utilizzare policy basate sulle identità in IAM. Le Policy di affidabilità sono policy basate su risorse collegate a un ruolo che definisce quali principali assumono il ruolo. Quando crei un ruolo in IAM, il ruolo deve avere due elementi: una politica di fiducia che indichi chi può assumere il ruolo e una politica di autorizzazione che indichi cosa può fare con quel ruolo. Ricorda che l'aggiunta di un account alla policy di affidabilità di un ruolo è solo una parte della procedura per stabilire la relazione di fiducia. Per impostazione predefinita, gli utenti negli account attendibili non possono assumere il ruolo fino a quando l'amministratore dell'account non concede agli utenti l'autorizzazione ad assumere il ruolo.

L'Marketplace AWS Image Building Service utilizza due ruoli IAM e ogni ruolo ha una politica di autorizzazioni e una politica di fiducia. Se hai utenti che accedono al Marketplace AWS sito Web per creare immagini private, tali utenti necessitano anche delle autorizzazioni IAM per elencare e assegnare i ruoli necessari per creare e visualizzare le immagini private che creano.

In qualità di amministratore, crei i due ruoli richiesti e le relative politiche associate. Il primo ruolo è un [profilo di istanza](#) collegato all'istanza creata durante il processo di creazione dell'immagine. Un profilo dell'istanza è un container per un ruolo IAM che puoi utilizzare per inoltrare informazioni

sul ruolo a un'istanza Amazon EC2 quando questa viene avviata. Il secondo è un ruolo IAM che fornisce l'accesso [AWS Systems Manager](#) ad Amazon EC2. Per configurare il profilo dell'istanza, allega una politica di autorizzazioni che fornisca le autorizzazioni richieste. Quindi modificare la policy di attendibilità per il ruolo per consentire ad Amazon EC2 e Systems Manager di assumere tale ruolo.

Creazione di un ruolo del profilo dell'istanza

Per creare il ruolo del profilo dell'istanza tramite la console IAM

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione della console IAM, scegli Ruoli e quindi Crea ruolo.
3. Per Select type of trusted entity (Seleziona tipo di entità attendibile), scegli Servizio AWS.
4. In Scegli il servizio che utilizzerà questo ruolo, scegli EC2, quindi scegli Avanti: Autorizzazioni.
5. Per Crea politica, scegli Avanti: Revisione.
6. Per Nome del ruolo, specifica un nome del ruolo o un suffisso del nome del ruolo per facilitare ad esempio **MyInstanceRole** lo scopo di questo ruolo. I nomi di ruoli devono essere univoci nell'Account AWS.
7. Rivedere il ruolo e scegliere Crea ruolo.
8. Nella pagina Ruoli, scegli il ruolo che hai creato.
9. Per le autorizzazioni, scegli Aggiungi politica in linea.
10. Scegli la scheda JSON e sostituisci tutto il testo con il InstanceRolePermissionsPolicy testo seguente.

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

```

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

```

Note

Prima di iniziare questo processo, devi creare il bucket S3, DOC-EXAMPLE-BUCKET.

11.Scegli Review policy (Esamina policy).

12. Per Nome della politica, inserisci un nome che ti aiuti a identificare lo scopo di questa politica, ad esempio **MyInstanceRolePolicy**, e scegli Crea politica.

Per modificare la relazione di attendibilità per il ruolo

1. Nella pagina Ruoli, scegli il ruolo che hai creato.
2. Scegli la scheda Relazioni di fiducia, quindi scegli Modifica relazione di fiducia.
3. Selezionate tutto il testo nella casella di testo del documento di politica e sostituitelo con il `InstanceRoleTrustPolicy` testo seguente.

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

4. Scegli Update Trust Policy (Aggiorna policy di trust).

Creazione di un ruolo AWS Systems Manager di automazione

Per creare il ruolo AWS Systems Manager di automazione

1. Nel pannello di navigazione della console IAM, scegli Ruoli e quindi Crea ruolo.
2. Per Select type of trusted entity (Seleziona tipo di entità attendibile), scegli Servizio AWS.
3. In Scegli il servizio che utilizzerà questo ruolo, scegli EC2, quindi scegli Avanti: Autorizzazioni.
4. Per Crea politica, scegli Avanti: Revisione.
5. Per Nome del ruolo, specifica un nome del ruolo o un suffisso del nome del ruolo per facilitare ad esempio **MyAutomationRole** lo scopo di questo ruolo. I nomi di ruoli devono essere univoci nell'Account AWS.

6. Rivedere il ruolo e scegliere Crea ruolo.
7. Nella pagina Ruoli, scegli il ruolo che hai creato.
8. Per le autorizzazioni, scegli Aggiungi politica in linea.
9. Scegli la scheda JSON e sostituisci tutto il testo con il AutomationRolePermissionsPolicy testo seguente.

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

```

        "Effect": "Allow"
      }
    ]
  }

```

Note

È necessario sostituire `{{ Instance Profile }}` con Amazon Resource Name (ARN) per il ruolo di policy dell'istanza creato in precedenza. Individua il ruolo nella console di gestione IAM e scegliilo. Nella pagina di riepilogo del ruolo, l'ARN del ruolo è il primo elemento elencato, `arn:aws:iam::123456789012:role/MyInstanceRole` ad esempio.

Per modificare la relazione di attendibilità per il ruolo

1. Nella pagina Ruoli, scegli il ruolo che hai creato.
2. Scegli la scheda Relazioni di fiducia, quindi scegli Modifica relazione di fiducia.
3. Sostituisci tutto il testo nella casella di testo del documento di politica con il `InstanceRoleTrustPolicy` testo seguente.

```

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

```

4. Scegli Update Trust Policy (Aggiorna policy di trust).

Ora hai creato i due ruoli e le politiche associate che utilizzerai durante il processo di creazione dell'immagine privata.

Utilizzo di una politica per accedere al Marketplace AWS sito Web

La maggior parte delle organizzazioni non consente agli utenti di accedere con le credenziali dell'account root. Invece, creano utenti con autorizzazioni limitate in base a ruoli organizzativi o attività che solo determinate persone possono eseguire. Marketplace AWS fornisce due policy principali gestite da IAM per l'utilizzo Marketplace AWS degli strumenti. Utilizza queste due politiche gestite per fornire la possibilità di eseguire le attività descritte:

- `AWSMarketplaceFullAccess`— Fornisce la possibilità di abbonarsi e annullare l'iscrizione al software IAM, consente agli utenti di gestire le istanze Marketplace AWS software dalla pagina Il Marketplace AWS tuo software e fornisce l'accesso amministrativo ad Amazon EC2.
- `AWSMarketplaceRead-only`— Fornisce la possibilità di rivedere AWS gli abbonamenti.

Puoi aggiungere la politica `AWSMarketplaceFullAccess` gestita a un utente, un gruppo o un ruolo per fornire tutte le autorizzazioni necessarie per accedere al Marketplace AWS sito Web ed eseguire le attività associate a Marketplace AWS Private Image Build.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creating a role for a third-party identity provider \(federation\)](#) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina [Creating a role for an IAM user](#) (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente di IAM.

La prossima volta che un utente o un membro di un gruppo o ruolo selezionato accede al Marketplace AWS sito Web, può eseguire le attività associate al processo di creazione dell'immagine privata.

Creare un'immagine privata

Important

Marketplace AWS interromperà il metodo di consegna di Private Image Build nell'aprile 2024. Il metodo di consegna è disponibile solo per gli abbonati esistenti fino alla sua sospensione. Per ulteriori informazioni, consulta [Creazione di immagini private](#).

Quando crei un'immagine privata, selezioni il pacchetto software Marketplace AWS e l'Amazon Machine Image (AMI) di base nella tua console Amazon Elastic Compute Cloud (Amazon EC2) che utilizzerai per creare la nuova immagine privata. Prima di iniziare il processo di compilazione è necessario configurare AWS l'ambiente in modo da poter fornire:

- L'ID AMI per l'immagine di base su cui installerai il Marketplace AWS prodotto.
- Il nome di un bucket Amazon Simple Storage Service (Amazon S3) per archiviare i registro delle build. Il bucket S3 deve trovarsi nel bucket S3 deve trovarsi nel Regione AWS bucket S3 deve trovarsi nella stessa.
- Il profilo dell'istanza Amazon EC2 con cui verrà installato il pacchetto (vedi la sezione precedente).
- Il ruolo di automazione AWS Identity and Access Management (IAM) che il processo di creazione dell'immagine utilizzerà per creare l'AMI (vedere la sezione precedente).
- Il nome della nuova immagine privata.

Se hai esperienza nell'uso Servizi AWS, probabilmente conosci la scelta Regioni AWS, la ricerca dell'ID AMI sulla dashboard di Amazon EC2 e l'utilizzo dei bucket Amazon S3.

Per trovare un prodotto che supporti la creazione di un'immagine privata, vai alla [pagina di ricerca del Marketplace AWS prodotto](#) e, per il filtro di ricerca del metodo di consegna, scegli Immagine privata di Amazon Machine. Dalla pagina dei dettagli del prodotto, puoi configurare le opzioni di approvvigionamento, configurazione ed evasione. Il prodotto che crei viene aggiunto al tuo Account AWS.

Oltre ai prerequisiti specificati nella sezione precedente, l'AMI di base deve soddisfare i seguenti requisiti:

- LinuxLe AMI devono avere Wget o essere cURL installate e configurate. Windows Le AMI devono essere PowerShell installate.
- LinuxLe AMI devono essere in grado di eseguire gli [script EC2 User Data](#) o avere l'AWS Systems Manager agente (agente SSM) preinstallato.
- WindowsLe AMI devono avere l'agente SSM preinstallato.

Per creare un'immagine privata

1. Nella pagina [Marketplace AWS](#) dei dettagli del prodotto, scegli Continua per abbonarti.
2. Nella pagina Iscriviti a questo software, in Termini e condizioni, scegli Mostra dettagli per visualizzare il tipo di istanza del prodotto, i costi di utilizzo del software e il contratto di licenza con l'utente finale (EULA). A seconda del prodotto, potresti visualizzare diversi tipi di abbonamenti. Dopo aver scelto il tipo di abbonamento, scegli Accetta termini.
3. Scegli Continue to Configuration (Passa alla configurazione).
4. Nella pagina Configura questo software, per Opzione di gestione, scegli Private Amazon Machine Image.
5. Nella sezione Immagine privata, per 1. Scegli una regione, scegli la tua regione. Per 2. Scegli un'immagine privata da lanciare, scegli Crea nuova immagine privata.
6. Nella sezione Crea nuova immagine privata, per Seleziona un'AMI di base da utilizzare, scegli Posseduta da me, Immagini pubbliche o Immagini private.
 - a. Di mia proprietà: AMI che sono specificamente di tua proprietà Account AWS
 - b. Immagini pubbliche: AMI condivise con tutti Account AWS
 - c. Immagini private: AMI condivise con Account AWS
7. Per l'ID AMI di base pubblica o l'ID AMI di base privata di Input, inserisci l'ID AMI o usa la console Amazon EC2 per copiare e incollare l'ID AMI dell'immagine che desideri utilizzare come AMI di base.
8. Per Instance Profile, scegli il ruolo dell'istanza che hai creato come passaggio prerequisito.
9. Per Automation Role, scegli il ruolo di automazione che hai creato come passaggio prerequisito.
10. Per Build Logs, digita il nome di un bucket Amazon S3 in cui desideri archiviare i log. Questo è il nome del bucket semplice, ad esempio *DOC-EXAMPLE-BUCKET*, anziché il nome DNS completo.
11. In Nome immagine privata, digita il nome della nuova immagine privata.

Ti consigliamo di utilizzare una convenzione di denominazione per le immagini private che crei per renderle più facili da identificare. Inoltre, quando Marketplace AWS Image Building Service crea una nuova immagine privata, aggiunge un tag `AWSMarketplaceFulfillmentID`, che può essere utile per identificare successivamente le immagini private. Puoi anche completare i seguenti passaggi opzionali per fornire ulteriori dettagli oppure puoi avviare il processo di creazione scegliendo **Avvia creazione**.

(Facoltativo) Per fornire ulteriori dettagli sull'immagine privata

1. In **Note descrittive**, inserisci tutte le informazioni pertinenti che desideri includere per l'istanza che verrà utilizzata durante la creazione dell'immagine privata.
2. Per **Tipo di istanza**, scegli il tipo di istanza che desideri utilizzare per creare l'immagine privata.
3. Per **VPC**, scegli il VPC che desideri che l'istanza utilizzi durante la creazione dell'immagine privata, quindi scegli il gruppo di sicurezza e la sottorete.
4. Per **Abilita il sistema di notifica semplice**, scegli un argomento esistente o creane uno nuovo per ricevere notifiche quando lo stato della build cambia.
5. Scegli **Start Build**.

Il completamento del processo di creazione richiede 1—2 ore. Prendere nota delle seguenti informazioni sul processo:

- I costi per i servizi utilizzati durante il processo di creazione verranno visualizzati nella **Account AWS** sezione **used to start the private image build process**. Ciò include l'istanza che viene eseguita durante l'installazione Marketplace AWS del prodotto sull'immagine privata e il bucket S3 utilizzato per i log.
- È possibile visualizzare lo stato del processo di creazione o ricevere messaggi Amazon Simple Notification Service (Amazon SNS).
- Una volta completata la build, la nuova immagine privata viene aggiunta alla tua **Account AWS** ed è disponibile tramite la console Amazon EC2 come AMI elencata in **Owned by me**.
- I repository utilizzati per completare il processo di compilazione devono essere locali.
- Durante la compilazione, il processo blocca l'accesso a Internet.

Utilizzo di alias AMI

Un'Amazon Machine Image (AMI) viene identificata con un AMI ID. Puoi utilizzare il plugin `ami-id` per indicare quale AMI utilizzare al lancio di un prodotto. L'AMI ID ha il modulo `ami-<identificatore>` ad esempio, `ami-123 esempio 456`. Ogni versione di ogni prodotto in ogni Regione AWS ha un'AMI diversa (e diverso AMI ID).

Avvio di un prodotto da Marketplace AWS, il AMI ID viene compilato automaticamente. Avvio del AMI ID è utile se si desidera automatizzare il lancio di prodotti da AWS Command Line Interface (AWS CLI) o utilizzando Amazon Elastic Compute Cloud (Amazon EC2). Puoi trovare il AMI ID quando configuri il software al momento del lancio. Per ulteriori informazioni, consulta la pagina [Fase 3: Configurazione del software](#).

La `ami-alias` anche nella stessa posizione del AMI ID, durante la configurazione del software. La `ami-alias` è un ID simile al AMI ID, ma è più facile da usare nell'automazione. Un record `ami-alias` ha il modulo `aws/service/marketplace/prod-<identificatore>/<versione>` ad esempio, `aws/service/marketplace/prod-1234example5678/12.2`. È possibile usare questa `ami-alias-id` in qualsiasi regione e AWS lo mappa automaticamente alla regione corretta AMI ID.

Utilizzo della versione più recente di un prodotto utilizzare il termine `latest` al posto della versione nella `ami-alias` AWS scegliere la versione più recente del prodotto, ad esempio, `aws/service/marketplace/prod-1234example5678/latest`.

Warning

Utilizzo di `latest` L'opzione fornisce la versione del software rilasciata più recente. Tuttavia, utilizzare questa funzione con cautela. Ad esempio, se un prodotto ha le versioni 1.x e 2.x disponibili, è possibile che tu stia utilizzando la versione 2.x. Tuttavia, la versione più recente del prodotto potrebbe essere una correzione di bug per 1.x.

Esempi di utilizzo di alias AMI

Gli alias AMI sono utili nell'automazione. poiché possono essere utilizzati nella AWS CLI o in AWS CloudFormation Modelli di Modelli.

Il seguente esempio illustra l'utilizzo di un alias AMI per avviare un'istanza utilizzando il AWS CLI.

```
aws ec2 run-instances
```

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

Il seguente esempio mostra un CloudFormation modello che accetta l'alias AMI come parametro di input per creare un'istanza.

```
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
```

Prodotti container

I prodotti container sono prodotti autonomi realizzati come immagini di container. I prodotti container possono essere gratuiti o devono essere pagati utilizzando un'opzione di prezzo fornita dal venditore. I prodotti container possono essere utilizzati con più runtime e servizi di container, tra cui [Amazon Elastic Container Service](#) (Amazon ECS), [Amazon Elastic Kubernetes Service \(Amazon EKS\)](#) e persino servizi in esecuzione sulla tua infrastruttura. Per un elenco completo dei runtime e dei servizi supportati con ulteriori informazioni su ciascuno di essi, consulta [Servizi supportati per prodotti container](#)

Puoi scoprire, abbonarti e distribuire prodotti container sul Marketplace AWS sito Web o nella console Amazon ECS. Puoi distribuire molti prodotti su Amazon ECS o Amazon EKS utilizzando modelli di distribuzione forniti dal venditore, come le definizioni delle attività o i grafici Helm. In alternativa, puoi accedere alle immagini dei container direttamente dai repository privati di [Amazon Elastic Container Registry](#) (Amazon ECR) dopo aver sottoscritto tali prodotti.

Se un prodotto è abilitato QuickLaunch, puoi utilizzarlo per testare rapidamente i prodotti container su un cluster Amazon EKS con pochi passaggi. QuickLaunch utilizza AWS CloudFormation per creare un cluster Amazon EKS e avviare il software del contenitore su di esso. Per ulteriori informazioni sull'avvio con QuickLaunch, consulta [QuickLaunch in Marketplace AWS](#).

Questa sezione fornisce informazioni sulla ricerca, la sottoscrizione e il lancio di prodotti container in Marketplace AWS

Modelli di prezzo per i prodotti container a pagamento

I prodotti container a pagamento devono avere uno o più modelli di prezzo. Come per tutti gli altri prodotti a pagamento Marketplace AWS, i prodotti in container a pagamento ti vengono fatturati AWS in base al modello di prezzo. Il modello di prezzo potrebbe essere una tariffa mensile fissa o un prezzo orario, monitorato in pochi secondi e ripartito proporzionalmente. I dettagli sui prezzi verranno visualizzati nella pagina prodotto e al momento dell'abbonamento al prodotto.

I modelli di prezzo supportati per i prodotti in container Marketplace AWS sono i seguenti:

- Un canone mensile fisso che offre un utilizzo illimitato.
- Un addebito anticipato per l'utilizzo del prodotto per la durata di un contratto a lungo termine.
- Un pay-as-you-go modello (in genere su base oraria) basato sull'utilizzo del prodotto.
- Un pay-up-front modello con prezzi contrattuali.

Per maggiori informazioni su ciascun modello, consulta [i prezzi dei prodotti Container](#) nella Guida al Marketplace AWS venditore.

Panoramica dei container e di Kubernetes

I contenitori, come i contenitori [Docker](#), sono una tecnologia software open source che fornisce un ulteriore livello di astrazione e automazione rispetto ai sistemi operativi virtualizzati come Linux e Windows Server. Proprio come le macchine virtuali sono istanze di immagini di server, i contenitori sono istanze di immagini di contenitori Docker. Racchiudono il software applicativo server in un file system che contiene tutto ciò di cui ha bisogno per l'esecuzione: codice, runtime, strumenti di sistema, librerie di sistema e così via. Con i contenitori, il software funziona sempre allo stesso modo, indipendentemente dall'ambiente in cui si trova.

Analogamente alle macchine virtuali Java, i container richiedono una piattaforma sottostante che fornisca un livello di traduzione e orchestrazione pur essendo isolati dal sistema operativo e dagli

altri. Esistono diversi servizi di runtime e orchestrazione compatibili con Docker che puoi utilizzare con i contenitori Docker, tra cui Amazon ECS, un servizio di orchestrazione altamente scalabile e ad alte prestazioni per AWS, e Amazon EKS, che semplifica la distribuzione, la gestione e la scalabilità di applicazioni containerizzate utilizzando [Kubernetes](#), un servizio di gestione e orchestrazione open source.

Ricerca e abbonamento ai prodotti container

I prodotti container sono prodotti Marketplace AWS che possono essere lanciati su immagini di container. I prodotti container includono qualsiasi prodotto Marketplace AWS in cui il venditore ha fornito un'opzione di evasione con un'immagine del contenitore, una tabella Helm o un metodo di spedizione aggiuntivo per Amazon EKS. Per ulteriori informazioni sui metodi di consegna dei prodotti in container, consulta [Metodi di consegna dei prodotti in container](#)

Molti ambienti di lancio, noti anche come servizi supportati, sono disponibili per le opzioni di evasione degli ordini relativi ai prodotti container. Gli ambienti di lancio includono servizi come Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e persino la tua infrastruttura autogestita. Per un elenco completo degli ambienti di lancio dei prodotti container disponibili, consulta [Servizi supportati per prodotti container](#)

Sfoggia i prodotti container utilizzando il Marketplace AWS sito Web

Puoi sfogliare i prodotti in contenitore utilizzando il [Marketplace AWS sito Web](#).

Per sfogliare i prodotti in contenitore utilizzando il Marketplace AWS sito Web

1. Vai alla [pagina Marketplace AWS di ricerca](#).
2. Filtra il metodo di consegna per immagine del contenitore o grafico Helm.
3. (Facoltativo) Filtra i servizi supportati per restringere i risultati della ricerca in base ai servizi con cui è possibile lanciare il prodotto.

Dopo aver trovato un prodotto che ti interessa, scegli il titolo per accedere alla pagina dei dettagli del prodotto.

Pagina dei dettagli del prodotto Container

Nella pagina dei dettagli del prodotto in Marketplace AWS, puoi trovare i dettagli sul prodotto, incluse le seguenti informazioni:

- **Panoramica del prodotto:** la panoramica include una descrizione del prodotto e le seguenti informazioni:
 - La versione del prodotto che stai visualizzando.
 - Un link al profilo del venditore.
 - Le categorie di prodotti a cui appartiene questo prodotto.
 - I sistemi operativi supportati per eseguire questo software.
 - I metodi di consegna disponibili per l'avvio del software.
 - I servizi supportati su cui è possibile lanciare questo prodotto.
- **Informazioni sui prezzi:** i prodotti hanno piani gratuiti, Bring Your Own License (BYOL), pay-up-front con prezzi contrattuali, pay-as-you-go con un prezzo fisso mensile o annuale o un prezzo orario. [Per ulteriori informazioni sui modelli di prezzo, consulta i prezzi dei prodotti Container.](#)
- **Informazioni sull'utilizzo:** qui sono incluse le opzioni di adempimento fornite dal venditore con istruzioni per avviare ed eseguire il software. Ogni prodotto deve avere almeno un'opzione di evasione ordini e può averne fino a cinque. Ogni opzione di evasione degli ordini include un metodo di consegna e istruzioni da seguire per avviare ed eseguire il software.
- **Informazioni sull'assistenza:** questa sezione include dettagli su come ottenere assistenza per il prodotto e sulla relativa politica di rimborso.
- **Recensioni dei clienti:** trova le recensioni sul prodotto di altri clienti o scrivi le tue.

Per abbonarti a un prodotto, scegli Continua con l'abbonamento nella pagina dei dettagli del prodotto. Per ulteriori informazioni sull'abbonamento ai prodotti, consulta [scrizione ai prodotti in Marketplace AWS](#).

Iscrizione ai prodotti in Marketplace AWS

Per utilizzare un prodotto, devi prima abbonarti. Nella pagina di abbonamento, puoi visualizzare le informazioni sui prezzi dei prodotti a pagamento e accedere al contratto di licenza con l'utente finale (EULA) per il software.

Per un prodotto con prezzi contrattuali relativi ai container, seleziona il prezzo del contratto e scegli Accetta contratto per procedere. In questo modo viene creato un abbonamento al prodotto, che dà diritto all'uso del software. Il completamento dell'abbonamento richiederà uno o due minuti. Dopo aver ricevuto il diritto a un prodotto a pagamento, ti verrà addebitato l'importo quando inizi a utilizzare il software. Se annulli l'abbonamento senza interrompere tutte le istanze in esecuzione del software, continuerai a ricevere i costi per l'utilizzo del software. Potrebbero inoltre essere addebitati costi di

infrastruttura correlati all'utilizzo del prodotto. Ad esempio, se crei un nuovo cluster Amazon EKS per ospitare il prodotto software, ti verrà addebitato il servizio.

Note

Per una procedura dettagliata su come abbonarsi e distribuire un prodotto basato su container, puoi anche fare riferimento ai seguenti video:

- [Distribuzione di Marketplace AWS contenitori su cluster Amazon ECS \(3:34\)](#)
- [Distribuzione di prodotti Marketplace AWS basati su container utilizzando Amazon ECS Anywhere \(5:07\)](#)
- [Gestione dei componenti aggiuntivi di Amazon EKS](#)

Metodi di consegna dei prodotti in container

Un prodotto in imballaggio Marketplace AWS è considerato un prodotto container se il venditore ha fornito almeno un'opzione di evasione con un'immagine del contenitore, una tabella Helm o un componente aggiuntivo per il metodo di spedizione Amazon EKS.

Metodo di consegna dell'immagine del contenitore

Per un'opzione di evasione con un metodo di spedizione basato sull'immagine del contenitore, utilizza le istruzioni fornite dal venditore per lanciare il prodotto. Questa operazione viene eseguita estraendo le immagini Docker direttamente dal registro su Amazon Elastic Container Marketplace AWS Registry. Per ulteriori informazioni sull'avvio con questo metodo di distribuzione, consulta [Avvio con un'opzione di evasione dell'immagine Container](#)

Metodo di consegna di Helm chart

Per un'opzione di evasione degli ordini con un metodo di spedizione Helm chart, utilizza le istruzioni o il modello di implementazione forniti dal venditore per lanciare il prodotto. Questo viene fatto installando un grafico Helm utilizzando la CLI di Helm. Puoi avviare l'applicazione su un cluster Amazon EKS esistente o un cluster autogestito su EKS Anywhere Amazon Elastic Compute Cloud (Amazon EC2) o in locale. Per ulteriori informazioni sull'avvio con questo metodo di distribuzione, consulta [Lancio con un'opzione Helm Fulfillment](#)

Componente aggiuntivo per il metodo di consegna Amazon EKS

Per un'opzione di evasione degli ordini con un componente aggiuntivo per il metodo di consegna Amazon EKS, utilizza la console Amazon EKS o la CLI di Amazon EKS per lanciare il prodotto. [Per ulteriori informazioni sui componenti aggiuntivi di Amazon EKS, consulta i componenti aggiuntivi di Amazon EKS.](#)

Servizi supportati per prodotti container

L'elenco seguente include tutti i servizi supportati per i prodotti container in Marketplace AWS. Un servizio supportato è un servizio o un ambiente container in cui è possibile lanciare il prodotto. Un prodotto container deve includere almeno un'opzione di evasione degli ordini che includa un metodo di consegna con istruzioni per il lancio in uno o più ambienti.

Amazon ECS

Amazon Elastic Container Service (Amazon ECS) è un servizio di gestione dei container veloce e altamente scalabile che puoi utilizzare per eseguire, arrestare e gestire i container su un cluster. I container sono definiti in una definizione di attività utilizzata per eseguire singoli processi o processi all'interno di un servizio. In questo contesto, un servizio è una configurazione che consente di eseguire e gestire un numero specifico di attività contemporaneamente in un cluster. Puoi eseguire processi e servizi su un'infrastruttura serverless gestita da AWS Fargate. In alternativa, per un maggiore controllo sull'infrastruttura, puoi eseguire i tuoi processi e i tuoi servizi su un cluster di istanze Amazon EC2 gestite da te.

Per ulteriori informazioni su Amazon ECS, consulta [What is Amazon Elastic Container Service](#) nella Amazon Elastic Container Service Developer Guide.

Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) è un servizio gestito che semplifica l'uso di Kubernetes su AWS, senza la necessità di installare, eseguire o gestire il piano di controllo o i nodi Kubernetes. Kubernetes è un sistema open source per automatizzare l'implementazione, il dimensionamento e la gestione di applicazioni containerizzate.

Puoi cercare, abbonarti e distribuire software Kubernetes di terze parti utilizzando la console Amazon EKS. Per ulteriori informazioni, consulta [Managing Amazon EKS add-ons nella Amazon EKS User Guide](#).

Kubernetes autogestito

Puoi lanciare prodotti container su cluster Kubernetes autogestiti in esecuzione in Amazon ECSEKS Anywhere, Anywhere Amazon EC2 o su un'infrastruttura locale.

Amazon ECS Anywhere è una funzionalità di Amazon ECS che puoi utilizzare per eseguire e gestire carichi di lavoro in container su un'infrastruttura gestita dal cliente. Amazon ECS si Anywhere basa su Amazon ECS per fornire un'esperienza coerente di strumenti e API in tutte le applicazioni basate su contenitori.

Per ulteriori informazioni, consulta [Amazon ECS Anywhere](#).

EKS Anywhere è un servizio che puoi utilizzare per creare un cluster Amazon EKS su un'infrastruttura gestita dal cliente. Puoi implementarlo EKS Anywhere come ambiente locale non supportato o come ambiente di produzione di qualità che può diventare una piattaforma Kubernetes locale supportata.

Per ulteriori informazioni su EKS Anywhere, consulta la [documentazione su EKS Anywhere](#).

Esplora i prodotti container utilizzando la console Amazon ECS

Puoi trovare prodotti in container anche nella console Amazon ECS. Il pannello di navigazione contiene collegamenti per scoprire nuovi prodotti Marketplace AWS e visualizzare gli abbonamenti esistenti.

Annullamento di un abbonamento

Per annullare un abbonamento a un prodotto, utilizza la pagina Il tuo software.

Prodotti container con prezzi contrattuali

Alcuni venditori offrono prodotti software pubblici basati su container con un modello di prezzo contrattuale, in base al quale l'utente accetta di effettuare un pagamento anticipato una tantum per quantità discrete di licenze di accesso al prodotto software per una durata a tua scelta, fatturate in anticipo tramite il tuo Account AWS

Example dell'acquisto di diversi tipi di licenze in quantità diverse

Ad esempio, è possibile acquistare 10 licenze di accesso utente e 5 licenze amministrative per un anno. Puoi scegliere di rinnovare automaticamente le licenze.

Inoltre, alcune aziende offrono prodotti software privati basati su container con un modello di prezzo contrattuale. Un'offerta privata ha in genere una durata fissa che non è possibile modificare.

Puoi acquistare un contratto di prodotto software basato su container utilizzando la pagina dei dettagli del prodotto su Marketplace AWS. Se questa opzione è disponibile, nella pagina dei dettagli del prodotto viene visualizzato l'AMI con prezzi contrattuali per Metodo di consegna. Una volta effettuato l'acquisto, verrai indirizzato al sito Web del prodotto per la configurazione e la configurazione dell'account. I costi di utilizzo verranno quindi visualizzati nel normale Account AWS rapporto di fatturazione.

Abbonamento a un prodotto container con prezzo contrattuale, offerta pubblica in Marketplace AWS

Abbonarsi a un prodotto basato su container in offerta pubblica con un modello di prezzo contrattuale

Note

Per informazioni sull'abbonamento tramite Amazon EKS, consulta [Gestione dei componenti aggiuntivi di Amazon EKS](#).

1. Accedi Marketplace AWS e trova un prodotto software basato su container con un modello di prezzo contrattuale.
2. Nella pagina Approvvigionamento, visualizza le informazioni sui prezzi.

Puoi visualizzare le unità e la tariffa per ogni durata (in mesi).

3. Per iniziare l'abbonamento, scegli Continua con l'abbonamento.


Per salvare questo prodotto senza abbonarti, scegli Salva nella lista.

4. Crea un contratto esaminando le informazioni sui prezzi e configurando i termini del prodotto software.
 - a. Scegli la durata del contratto: 1 mese, 12 mesi, 24 mesi o 36 mesi.
 - b. In Impostazioni di rinnovo, scegli se rinnovare automaticamente il contratto.
 - c. In Opzioni di contratto, scegli una quantità per ogni unità.

Il prezzo totale del contratto viene visualizzato in Dettagli sui prezzi.

5. Dopo aver effettuato le selezioni, scegli Crea contratto.


Il prezzo totale del contratto viene addebitato all'utente Account AWS e viene generata una licenza. AWS License Manager

 Note

L'elaborazione dell'abbonamento e la generazione di una licenza nell'account License Manager per il prodotto software possono richiedere fino a 10 minuti.

Abbonamento a un prodotto container con prezzo contrattuale, offerta privata in Marketplace AWS

Abbonarsi a un prodotto basato su container con offerta privata con un modello di prezzo contrattuale

 Note

Per informazioni sull'abbonamento tramite Amazon EKS, consulta [Gestione dei componenti aggiuntivi di Amazon EKS](#).

1. Accedi Marketplace AWS con il tuo account acquirente.
2. Visualizza l'offerta privata.
3. Nella pagina Approvvigionamento, visualizza le informazioni sui prezzi.

Puoi visualizzare le unità e la tariffa per ogni durata (in mesi).

4. Scegli Continua a sottoscrivere per iniziare l'abbonamento.
5. Crea un contratto esaminando le informazioni sui prezzi e configurando i termini del prodotto software.

La durata del contratto è già stabilita dal venditore e non può essere modificata.

6. In Opzioni contrattuali, scegli una quantità per ogni unità.
7. Visualizza il prezzo totale del contratto in Dettagli sui prezzi.

Puoi anche vedere l'offerta pubblica selezionando Visualizza offerta in Altre offerte disponibili.

8. Dopo aver effettuato le selezioni, scegli Crea contratto.

Note

L'elaborazione dell'abbonamento e la generazione di una licenza nell'account License Manager per il prodotto software possono richiedere fino a 10 minuti.

Accesso al software

Per accedere al prodotto software basato su container

1. Sulla Marketplace AWS console, vai a **Visualizza abbonamento** e visualizza la licenza per il prodotto software.
2. Nella pagina **Approvvigionamento**:
 - a. Scegli **Gestisci licenza** per visualizzare, concedere l'accesso e monitorare l'utilizzo dei tuoi diritti in **AWS License Manager**.
 - b. Scegli **Continue to Configuration (Passa alla configurazione)**.
3. Nella pagina di avvio, visualizza i dettagli dell'immagine del contenitore e segui le istruzioni fornite.

Durante la creazione di un cluster Amazon Elastic Container Service (Amazon ECS), devi aggiungere AWS Identity and Access Management le seguenti autorizzazioni (IAM) alla tua policy 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": "*"
    }
  ]
}
```

}

Visualizzazione di una licenza generata

Per visualizzare una licenza generata

1. Accedi a AWS License Manager con il tuo Account AWS.
2. In Licenze concesse, visualizza tutte le licenze concesse.
3. Cerca le licenze inserendo lo SKU, il destinatario o lo stato del prodotto nella barra di ricerca.
4. Scegli l'ID della licenza e visualizza i dettagli della licenza.
5. È possibile visualizzare l'Emittente (AWS/Marketplace) e le Entitlements (le unità a cui la licenza concede il diritto di utilizzare, accedere o utilizzare un'applicazione o una risorsa).

Modifica di un contratto esistente

Se hanno già sottoscritto un impegno iniziale per un prodotto Container, Marketplace AWS gli acquirenti possono modificare alcuni aspetti del contratto. Un contratto Container è supportato da offerte basate su termini contrattuali anziché da offerte FCP (Flexible Consumption Pricing) su base oraria o annuale. Questa funzionalità è disponibile solo per le applicazioni integrate con AWS License Manager. Gli acquirenti possono acquistare licenze aggiuntive nell'ambito del diritto alla stessa offerta prevista dal contratto corrente. Tuttavia, gli acquirenti non possono ridurre il numero di licenze acquistate nel contratto. Gli acquirenti possono anche annullare il rinnovo automatico dell'abbonamento se l'opzione è abilitata dal venditore.

Note

Un'offerta contrattuale con programma di pagamento flessibile (FPS) non può essere modificata. L'acquirente non può modificare i diritti relativi a un contratto acquistato con FPS. Un diritto è il diritto di utilizzare, accedere o utilizzare un'applicazione o una risorsa. Le offerte FPS non sono modificabili.

Gestisci il tuo abbonamento

1. Sulla Marketplace AWS console, vai a Visualizza abbonamento e visualizza la licenza per il prodotto software.

2. Nella pagina Approvvigionamento, seleziona Gestisci licenza.
3. Dall'elenco, seleziona Visualizza termini.
4. Nella sezione Opzioni contrattuali, aumenta i tuoi diritti utilizzando le frecce. Non puoi ridurre il numero di diritti al di sotto dei diritti acquistati.
5. I dettagli del contratto e il prezzo totale vengono visualizzati nella sezione Dettagli sui prezzi.

Per annullare il rinnovo automatico dell'abbonamento

1. Sulla Marketplace AWS console, vai a Visualizza abbonamento e visualizza la licenza per il prodotto software.
2. Nella pagina Approvvigionamento, seleziona Gestisci licenza.
3. Nella pagina Abbonamento, individua la sezione Impostazioni di rinnovo.
4. Assicurati di aver compreso i termini e le condizioni relativi all'annullamento.
5. Seleziona la casella di controllo per annullare l'opzione di rinnovo automatico.

Avvio del software per container da Marketplace AWS

Dopo aver sottoscritto un abbonamento attivo a un prodotto container in Marketplace AWS, il passaggio successivo consiste nell'avviare il software. Per avviare il software, segui le istruzioni incluse in una delle opzioni di adempimento fornite dal venditore. In Marketplace AWS, un'opzione di adempimento è una procedura facoltativa fornita dal venditore per il lancio del prodotto nel tuo ambiente. Per i prodotti in container, il venditore può fornire fino a quattro opzioni di evasione, che possono utilizzare metodi di consegna diversi e rappresentare configurazioni diverse per il software. Ad esempio, un venditore potrebbe creare un'opzione di evasione degli ordini da utilizzare per testare il prodotto e un'altra da implementare su larga scala all'interno di un'azienda.

Puoi vedere quali opzioni di evasione sono disponibili nella sezione Informazioni d'uso della pagina dei dettagli del prodotto in Marketplace AWS. Ogni opzione di adempimento include informazioni sui servizi supportati e fornisce dettagli sulla versione del software. Esempi di servizi includono Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Kubernetes Service (Amazon EKS). Puoi scegliere Istruzioni d'uso per la documentazione fornita dal venditore su come utilizzare il prodotto, ad esempio su come accedere a un server Web o sulla configurazione post-lancio.

Note

Per una procedura dettagliata su come abbonarsi e distribuire un prodotto basato su container, puoi anche fare riferimento ai seguenti video:

- [Distribuzione di Marketplace AWS contenitori su cluster Amazon ECS \(3:34\)](#)
- [Distribuzione di prodotti Marketplace AWS basati su container utilizzando Amazon ECS Anywhere \(5:07\)](#)

[Distribuzione di prodotti basati su container AWS Marketplace utilizzando ECS Anywhere](#)

Avvia il software per container da Marketplace AWS

Per avviare il software contenitore da Marketplace AWS

1. Eseguire l'accesso ad [Marketplace AWS](#).
2. Sfoglia Marketplace AWS e trova il prodotto che contiene il software che desideri avviare. È necessario disporre di un abbonamento al prodotto per avviarne il software. Per informazioni su come trovare e abbonarsi ai prodotti container in Marketplace AWS, consulta [Ricerca e abbonamento ai prodotti container](#).
3. Scegli Continua con l'abbonamento nella pagina dei dettagli del prodotto.
4. Scegli Continue to Configuration (Passa alla configurazione). Se non vedi il pulsante, potresti dover prima accettare i termini oppure potresti non avere un abbonamento al prodotto.
5. In Opzione di evasione, seleziona un'opzione di evasione dall'elenco di opzioni fornito dal venditore. Dopo aver selezionato un'opzione di evasione ordini, puoi visualizzare i servizi che puoi lanciare nella sezione Servizi supportati. Per ulteriori informazioni sulle opzioni di evasione degli ordini, consulta [Opzioni di evasione dei prodotti containerizzati](#)
6. Scegli Continua al lancio.
7. Segui le istruzioni fornite dal venditore per lanciare il prodotto. Le istruzioni sono diverse per ogni opzione di adempimento. Per ulteriori informazioni, consultare [Avvio con un'opzione di evasione dell'immagine Container](#) o [Lancio con un'opzione Helm Fulfillment](#).
8. Facoltativo: scegli Istruzioni d'uso per visualizzare la documentazione fornita dal venditore su come configurare e utilizzare il prodotto dopo il lancio.

Opzioni di evasione dei prodotti containerizzati

Puoi vedere le opzioni di evasione disponibili nella sezione Informazioni d'uso della pagina dei dettagli di un prodotto. Oltre alle opzioni di evasione fornite dal venditore, Marketplace AWS include istruzioni per estrarre le immagini Docker direttamente da Amazon Elastic Container Registry (Amazon ECR).

Poiché le opzioni di evasione degli ordini sono fornite dal venditore, i relativi nomi e contenuti saranno diversi per ogni prodotto in vendita. Marketplace AWS. Sebbene i metodi siano unici per ogni prodotto e venditore, ogni opzione di evasione degli ordini deve avere un metodo di spedizione. Puoi pensare a un metodo di spedizione come a un tipo di opzione di evasione degli ordini. I tre metodi di consegna disponibili per i prodotti container sono Container image, Helm chart e Add on for Amazon EKS.

Avvio con un'opzione di evasione dell'immagine Container

Per un'opzione di evasione con un metodo di spedizione basato sull'immagine del contenitore, utilizza le istruzioni fornite dal venditore per lanciare il prodotto. Questa operazione viene eseguita estraendo le immagini Docker direttamente da Amazon ECR. I passaggi generali per lanciare il prodotto sono i seguenti:

1. Verifica di aver installato le versioni più recenti di AWS Command Line Interface (AWS CLI) e Docker. Per ulteriori informazioni, consulta [Using Amazon ECR with the AWS CLI](#) Amazon Elastic Container Registry User Guide.
2. Autentica il tuo client Docker nel tuo registro Amazon ECR. La procedura da seguire per eseguire questa operazione dipenderà dal sistema operativo in uso.
3. Estrai tutte le immagini Docker utilizzando l'immagine Amazon ECR fornita Amazon Resource Name (ARN). Per ulteriori informazioni, consulta la sezione [Estrazione di un'immagine](#) nella Amazon Elastic Container Registry User Guide.
4. Consulta le istruzioni d'uso o i link esterni forniti dal venditore per informazioni sull'uso del prodotto.

Lancio con un'opzione Helm Fulfillment

Per un'opzione di evasione degli ordini con un metodo di spedizione Helm, utilizza le istruzioni fornite dal venditore per lanciare il prodotto. Questo viene fatto installando un grafico Helm utilizzando la CLI di Helm. Puoi avviare l'applicazione su un cluster Amazon EKS esistente o un cluster autogestito su EKS Anywhere Amazon Elastic Compute Cloud (Amazon EC2) o in locale.

Note

L'ambiente di avvio deve utilizzare la versione 3.7.1 della CLI di Helm. [Per un elenco delle versioni di Helm, consulta le versioni di Helm su. GitHub](#)

Se il venditore lo ha abilitato QuickLaunch, puoi utilizzarlo per avviare l'applicazione. QuickLaunch è una funzionalità Marketplace AWS che consente di AWS CloudFormation creare un cluster Amazon EKS e avviare l'applicazione su di esso. Per ulteriori informazioni su QuickLaunch, consulta [QuickLaunch in Marketplace AWS](#).

Le istruzioni sono fornite dal venditore e sono diverse per ogni venditore e prodotto. I passaggi generali per lanciare un prodotto con un'opzione Helm Fulfillment sono i seguenti:

Per lanciare un prodotto con un'opzione Helm Fulfillment


1. Segui i passaggi da 1 a 6 di e scegli un'opzione di [Avvia il software per container da Marketplace AWS](#) evasione con un metodo di consegna basato sulla mappa Helm.
2. In Launch target, scegli l'ambiente in cui desideri eseguire la distribuzione:
 - Scegli Amazon managed Kubernetes per distribuire l'applicazione in Amazon EKS. Se il venditore l'ha abilitata QuickLaunch, puoi utilizzarla per creare un nuovo cluster Amazon EKS e avviarlo su di esso.
 - Scegli Kubernetes autogestito per distribuire l'applicazione in [EKS Anywhere](#) su qualsiasi cluster Kubernetes in esecuzione in Amazon EC2 o in locale.
3. Se esegui l'avvio in un cluster Kubernetes gestito da Amazon:
 - a. Per eseguire l'avvio su un cluster esistente in Amazon EKS, in Metodo di avvio, scegli Avvia su un cluster esistente e segui le istruzioni di avvio. Le istruzioni includono la creazione di un ruolo AWS Identity and Access Management (IAM) e il lancio dell'applicazione. Verifica di utilizzare la versione 3.7.1 della CLI di Helm.
 - b. Da utilizzare QuickLaunch per creare un nuovo cluster Amazon EKS e avviarlo su di esso, in Metodo di avvio, scegli Avvia su un nuovo cluster EKS con. QuickLaunch Scegli Launch per essere reindirizzato per creare uno stack nella AWS CloudFormation console. Questo stack creerà un cluster Amazon EKS e distribuirà l'applicazione installando il grafico Helm fornito dal venditore.
 - c. Nella pagina Quick create stack, in Stack name, fornisci un nome per questo stack.

- d. Esamine le informazioni nel riquadro Parametri e fornite tutte le informazioni necessarie. Esamina e seleziona i riconoscimenti in Capacità e scegli Crea stack.

 Note

Per ulteriori informazioni QuickLaunch, incluse informazioni sugli AWS CloudFormation stack e sul cluster Amazon EKS creato, consulta. [QuickLaunch in Marketplace AWS](#)

4. Se si avvia in un cluster Kubernetes autogestito:
 - a. Verifica di utilizzare la versione 3.7.1 della CLI di Helm.
 - b. Scegli Crea token per generare un token di licenza e un ruolo IAM. Questo token e ruolo vengono utilizzati per comunicare e AWS License Manager convalidare le autorizzazioni del prodotto.

 Note

Il numero massimo di token di licenza per un account è 10.

- c. Scegli Scarica come CSV per scaricare un file.csv con le informazioni sul token generato. Come per tutti i segreti e le password, archivia il file.csv in un luogo sicuro.
- d. Esegui i comandi in Salva come segreto Kubernetes per salvare il token di licenza e il ruolo IAM come segreti nel tuo cluster Kubernetes. Questo segreto viene utilizzato quando si installa il grafico Helm e si avvia l'applicazione. Marketplace AWS utilizza il segreto per verificare l'idoneità a questo prodotto.
- e. Esegui i comandi nell'applicazione Launch utilizzando il token per installare il grafico Helm che distribuisce l'applicazione nel tuo cluster.
- f. Scegli Istruzioni d'uso per la documentazione fornita dal venditore su come configurare e utilizzare il prodotto dopo il lancio.
- g. Facoltativo: utilizza i comandi forniti in [Opzionale] Scarica gli artefatti per scaricare localmente le immagini dei contenitori e i grafici Helm del prodotto.

Avvio con un'opzione di distribuzione Amazon EKS

Per un'opzione di evasione degli ordini con un componente aggiuntivo per il metodo di consegna Amazon EKS, utilizza la console Amazon EKS per distribuire il software sul tuo cluster Amazon EKS.

I passaggi generali per lanciare il prodotto sono i seguenti:

Per lanciare un prodotto con un'opzione di distribuzione Amazon EKS

1. Dopo esserti abbonato al prodotto, vai alla pagina di configurazione e scegli Continua con la console Amazon EKS per accedere alla console Amazon EKS.
2. Dalla console Amazon EKS, scegli Regione AWS dove viene distribuito il cluster. Seleziona il cluster in cui desideri distribuire il software.
3. Seleziona la scheda Componenti aggiuntivi.
4. Scegli Ottieni altri componenti aggiuntivi, scorri fino a individuare il componente aggiuntivo che desideri distribuire e scegli Avanti.
5. Seleziona la versione che desideri distribuire e scegli Avanti. Per ulteriori informazioni sulla distribuzione di Amazon EKS, consulta i [componenti aggiuntivi EKS](#).
6. Controlla le tue selezioni e scegli Crea.

QuickLaunch in Marketplace AWS

Se il venditore ha abilitato QuickLaunch un'opzione di evasione ordini, puoi utilizzarla per creare un cluster Amazon EKS e distribuirvi un'applicazione container. Con QuickLaunch, lo utilizzerai AWS CloudFormation per configurare e creare un cluster Amazon EKS e avviare un'applicazione contenitore su di esso. Con QuickLaunch, puoi avviare un'applicazione contenitore a scopo di test. Per utilizzarla QuickLaunch, segui la procedura riportata di seguito [Lancio con un'opzione Helm Fulfillment](#).

Per creare un cluster Amazon EKS su cui distribuire l'applicazione, crea uno CloudFormation stack. Uno stack è una raccolta di risorse di AWS che è possibile gestire come un'unità singola. Tutte le risorse di uno stack sono definite dal modello CloudFormation dello stack. Inoltre QuickLaunch, le risorse dello stack includono le informazioni necessarie per creare il cluster Amazon EKS e avviare l'applicazione. Per ulteriori informazioni sugli stacks in AWS CloudFormation, consulta [Working with stacks](#) nella Guida per l'AWS CloudFormation utente.

Dopo aver creato il cluster, QuickLaunch avvia l'applicazione installando sul cluster il grafico Helm fornito dal venditore. QuickLaunch lo gestisce per te come parte della creazione dello stack che crea anche il cluster Amazon EKS.

Prodotti per l'apprendimento automatico

Marketplace AWS ha una categoria di prodotti di machine learning a cui puoi abbonarti Marketplace AWS. La categoria di prodotto è Machine Learning. I prodotti di questa categoria includono pacchetti di modelli e algoritmi di machine learning (ML).

Puoi sfogliare e cercare centinaia di pacchetti di modelli e algoritmi ML da un'ampia gamma di sottocategorie, come visione artificiale, elaborazione del linguaggio naturale, riconoscimento vocale, testo, dati, voce, immagini, analisi video, rilevamento di frodi e analisi predittiva.

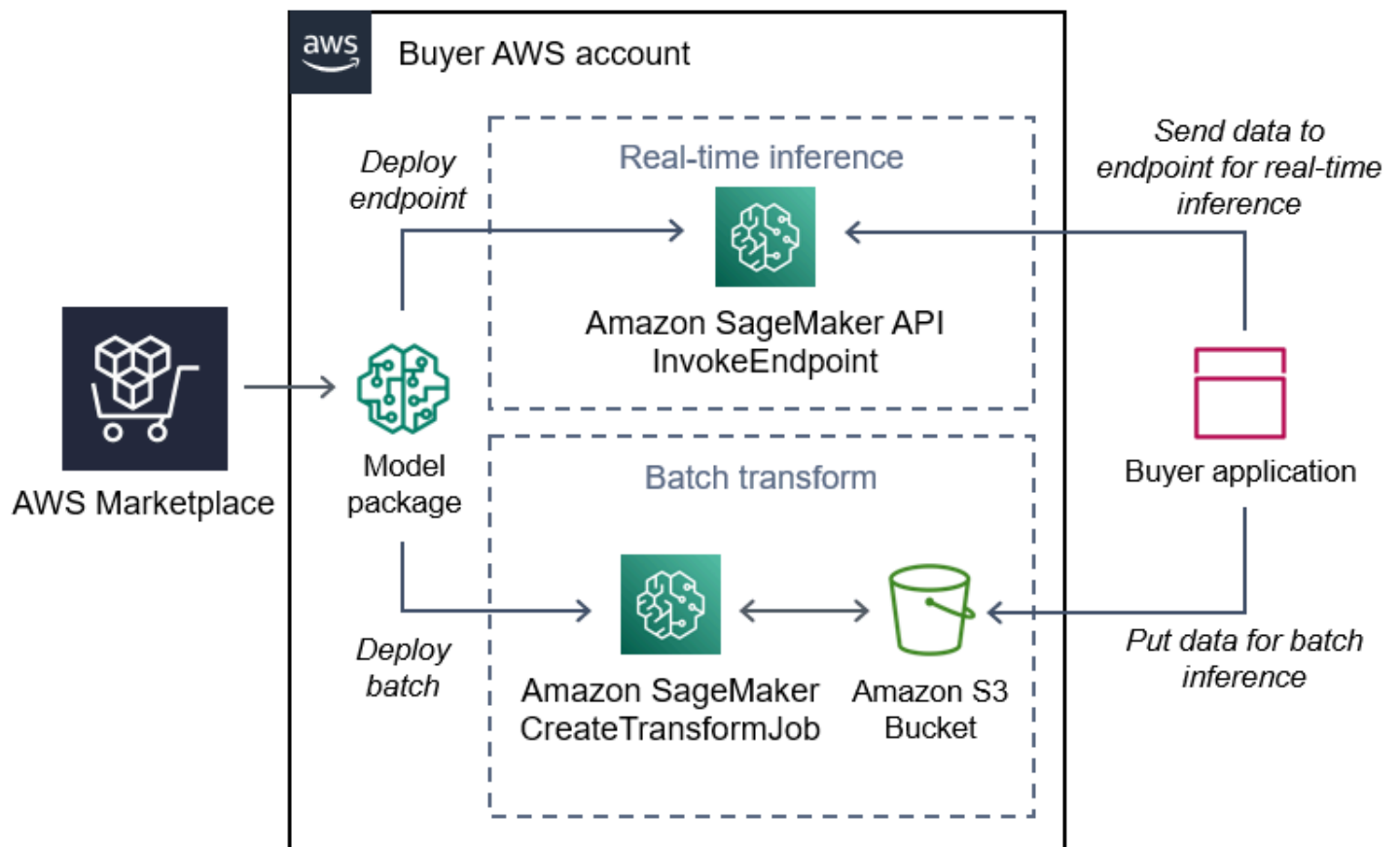
Per valutare la qualità e l'idoneità di un modello, puoi consultare le descrizioni dei prodotti, le istruzioni per l'uso, le recensioni dei clienti, esempi di [notebook Jupyter](#), i prezzi e le informazioni di assistenza. Puoi distribuire i modelli direttamente dalla SageMaker console Amazon, tramite un notebook Jupyter, con Amazon SDK o utilizzando SageMaker AWS Command Line Interface AWS CLI Amazon SageMaker fornisce un ambiente sicuro per eseguire i lavori di formazione e inferenza eseguendo una scansione statica su tutti i prodotti del marketplace.

Pacchetto SageMaker modello Amazon

Un pacchetto di SageMaker modelli Amazon è un modello ML preaddestrato unico identificato da un Amazon Resource Name (ARN) su Amazon. SageMaker I clienti utilizzano un pacchetto modello per creare un modello in Amazon. SageMaker Quindi, il modello può essere utilizzato con i servizi di hosting per eseguire inferenze in tempo reale o con la trasformazione in batch per eseguire l'inferenza in batch in Amazon. SageMaker

Il diagramma seguente mostra il flusso di lavoro per l'utilizzo di prodotti con pacchetti modello.

1. Su Marketplace AWS, puoi trovare e abbonarti a un prodotto con pacchetto modello.
2. Implementate il componente di inferenza del prodotto SageMaker per eseguire l'inferenza (o la previsione) in tempo reale o in batch.



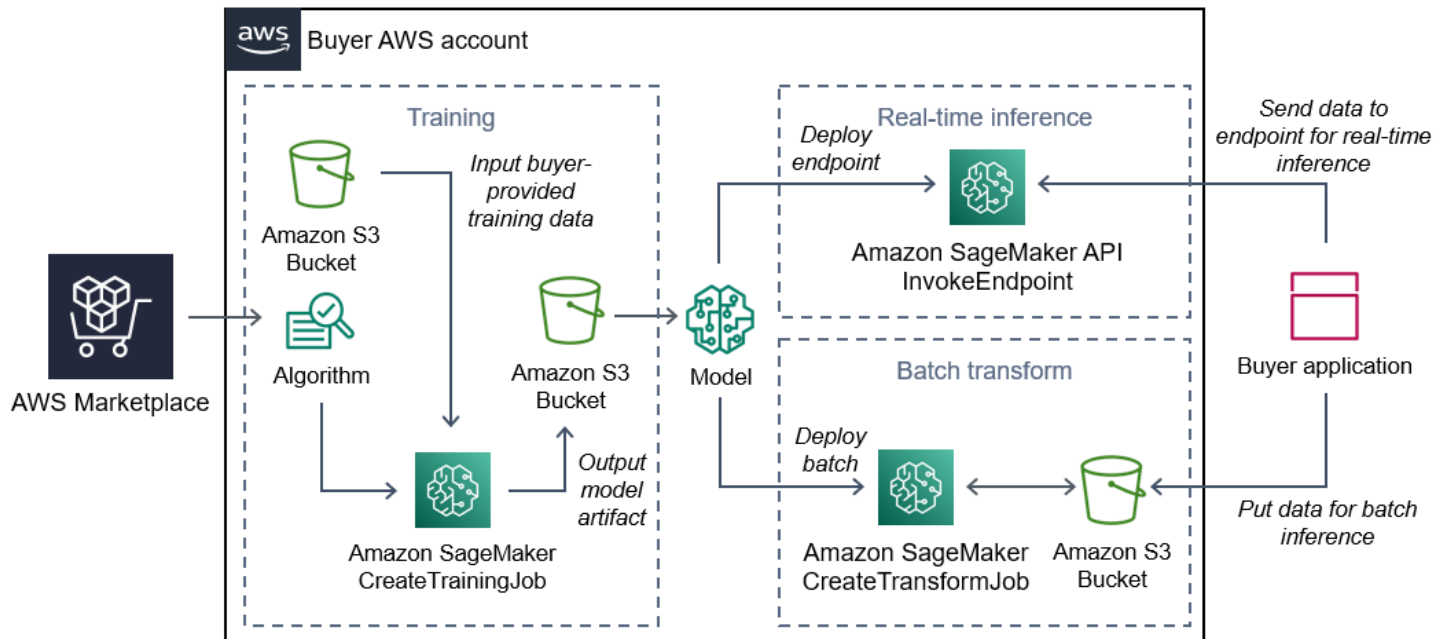
Algoritmo Amazon SageMaker

Un SageMaker algoritmo Amazon è un' SageMaker entità Amazon unica identificata da un ARN. Un algoritmo ha due componenti logiche: addestramento e inferenza.

Il diagramma seguente mostra il flusso di lavoro per l'utilizzo dei prodotti algoritmici.

1. Su Marketplace AWS, trovi e sottoscrivi un prodotto algoritmico.
2. Utilizzi il componente di formazione del prodotto per creare un lavoro di formazione o un lavoro di ottimizzazione utilizzando il set di dati di input in Amazon SageMaker per creare modelli di apprendimento automatico.
3. Una volta completato il componente di formazione del prodotto, genera gli artefatti del modello di apprendimento automatico.
4. SageMaker salva gli artefatti del modello nel tuo bucket Amazon Simple Storage Service (Amazon S3).

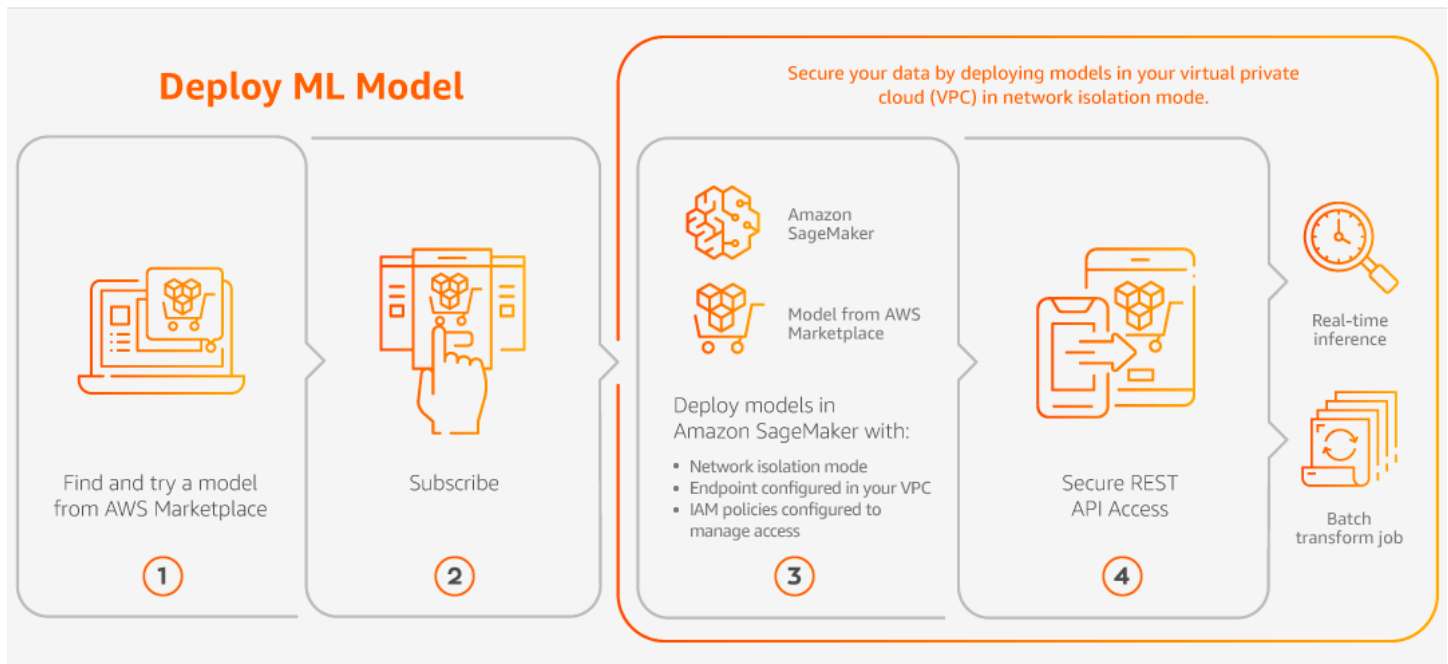
5. In SageMaker, puoi quindi implementare il componente di inferenza del prodotto utilizzando gli artefatti del modello generati per eseguire inferenze (o previsioni) in tempo reale o in batch.



Trova, sottoscrivi e distribuisce

Il diagramma seguente mostra una panoramica del processo per trovare, sottoscrivere e distribuire un prodotto di machine learning su Amazon. SageMaker

1. Trova e prova un modello da Marketplace AWS
2. Abbonati al prodotto ML
3. Implementa modelli in Amazon SageMaker
4. Usa API REST sicure
5. Esegui
 - Inferenza in tempo reale
 - Processo di trasformazione in batch



Paghi solo per l'utilizzo, senza commissioni minime o impegni anticipati. Marketplace AWS fornisce una fattura consolidata per gli algoritmi e i pacchetti di modelli e i costi di utilizzo AWS dell'infrastruttura.

Le seguenti sezioni spiegano come trovare, abbonarsi e distribuire un prodotto ML.

Argomenti

- [Trovare un prodotto per l'apprendimento automatico](#)
- [Abbonamento a un prodotto di machine learning](#)
- [Implementazione di un prodotto di machine learning](#)

Trovare un prodotto per l'apprendimento automatico

Per trovare pacchetti di SageMaker modelli e algoritmi Amazon

1. Accedi al [sito Web di AWS Marketplace](#).
2. In Trova Marketplace AWS prodotti che soddisfano le tue esigenze, utilizza il menu a discesa Categorie per trovare la sottocategoria in Machine Learning che ti interessa.
3. Puoi affinare i risultati della ricerca applicando filtri per tipo di risorsa, categoria e prezzo.
4. Dai risultati della ricerca, accedi alla pagina dei dettagli del prodotto.

5. Consulta la descrizione del prodotto, le istruzioni per l'uso, le recensioni dei clienti, i requisiti relativi ai dati, gli esempi di notebook Jupyter e le informazioni su prezzi e assistenza.

Abbonamento a un prodotto di machine learning

Per abbonarsi ai pacchetti SageMaker modello e agli algoritmi di Amazon

1. Dalla pagina dei dettagli del prodotto, scegli Continua per abbonarti.
2. Nella pagina di approvvigionamento, consulta le informazioni sui prezzi del prodotto e il contratto di licenza con l'utente finale (EULA).
3. Scegli Continua per abbonarti.

Implementazione di un prodotto di machine learning

Per distribuire pacchetti SageMaker modello e algoritmi Amazon

1. Conferma di disporre di un abbonamento valido all'algoritmo o al pacchetto modello accedendo a [Your Marketplace Software](#).
2. Configura il prodotto (ad esempio, selezionando una versione o una regione di distribuzione specifica) sul Marketplace AWS sito Web.

Dopo aver sottoscritto un prodotto Model Package o un prodotto algoritmico, il prodotto viene aggiunto all'elenco dei prodotti nella SageMaker console. Puoi anche utilizzare AWS gli SDK, il AWS Command Line Interface (AWS CLI) o la SageMaker console per creare un endpoint di inferenza REST completamente gestito o eseguire inferenze su batch di dati.

3. Visualizza la pagina dei dettagli SageMaker del prodotto Amazon scegliendo Visualizza in Amazon. SageMaker
4. Dalla SageMaker console Amazon, puoi distribuire i pacchetti modello e gli algoritmi utilizzando la SageMaker console Amazon, il notebook Jupyter, i comandi Amazon SageMaker CLI o le operazioni API.

[Per ulteriori informazioni sulla distribuzione su Amazon, consulta Getting Started. SageMaker](#)

Prodotti per servizi professionali

Marketplace AWS include prodotti che sono servizi professionali di Marketplace AWS rivenditori. Sono disponibili nella Servizi professionali categoria durante la ricerca in Marketplace AWS. Abbonati e acquisti questi prodotti tramite Marketplace AWS, ma collaborerai con il venditore per impostare i servizi professionali in base alle tue esigenze.

Acquisto di servizi professionali

È possibile ricercare servizi professionali utilizzando la Servizi professionali categoria in Marketplace AWS. Quando trovi un prodotto che ti interessa, richiedi un'offerta al venditore. Poiché i servizi professionali di solito implicano la collaborazione, è necessario fornire alcune informazioni aggiuntive al venditore per completare l'acquisto. Puoi anche usarlo come un'opportunità per negoziare i prezzi e qualsiasi altro dettaglio del servizio che deve essere risolto. Riceverai un'offerta privata per il prodotto. Per ulteriori informazioni sulle offerte private, consulta [Offerte private](#).

Per acquistare un prodotto di servizi professionali

1. Andare su [Marketplace AWS](#) e accedi al tuo AWS account, quindi cerca e trova un prodotto di servizi professionali che desideri acquistare.
2. Nella relativa pagina dei dettagli del prodotto, scegli Continua.
3. Sul Richiesta di assistenza, aggiungi le informazioni aggiuntive necessarie al venditore per creare l'offerta, inclusi nome, indirizzo e-mail, ragione sociale e qualsiasi informazione aggiuntiva utile al venditore, comprese le esigenze aziendali, le tempistiche e i requisiti contrattuali.
4. Il venditore ti contatterà tramite l'indirizzo e-mail che hai fornito per elaborare i dettagli della tua offerta. Una volta concordato, il venditore ti invierà un link all'offerta in Marketplace AWS. Apri il link in un browser e accedi al tuo AWS conto.
5. Controlla i dettagli dell'offerta nella pagina di approvvigionamento che hai aperto dal venditore. Assicurati che l'offerta sia per il servizio che ti aspetti e il prezzo che ti aspetti. Controlla anche i termini, indipendentemente dal fatto che tu paghi una somma forfettaria o una serie di addebiti. Se l'offerta è corretta, continua. In caso contrario, contatta il venditore per apportare modifiche.
6. UNDER Configura del contratto, scegli la configurazione che desideri utilizzare per il tuo contratto. Ad esempio, se si acquista un contratto di assistenza, potrebbero essere disponibili opzioni per Argento, Ori, oppure Platino contratti, con prezzi diversi.
7. Seleziona Create CONTRACT per acquistare il servizio. Il venditore deve contattarti entro 2 giorni lavorativi con le istruzioni per l'utilizzo del servizio.

Prodotti SaaS

Per i prodotti Software as a Service (SaaS), ti abboni ai prodotti tramite Marketplace AWS, ma accedi al prodotto nell'ambiente del venditore del software.

Argomenti

- [Modelli tariffari](#)
- [Avvio rapido](#)

Modelli tariffari

Marketplace AWS offre i seguenti modelli di prezzo.

Abbonamenti basati sull'utilizzo SaaS

Con gli abbonamenti SaaS basati sull'utilizzo, il venditore del software monitora l'utilizzo e paghi solo per quello che usi. Questo modello di pay-as-you-go prezzo è simile a quello di molti altri. Servizi AWS La fatturazione per l'utilizzo di un prodotto SaaS viene gestita tramite la AWS fattura.

Per abbonarsi utilizzando l'abbonamento SaaS basato sull'utilizzo

1. Nella pagina dei dettagli del prodotto, scegli Visualizza opzioni di acquisto per avviare la procedura di abbonamento.
2. Controlla l'abbonamento e scegli Abbonati nella pagina dell'abbonamento.

Note

Alcuni prodotti offrono un'opzione di implementazione Quick Launch, che riduce il tempo e le risorse necessari per configurare, distribuire e avviare il software. Questi prodotti sono identificati mediante un badge Quick Launch. Per ulteriori informazioni, consulta [the section called "Avvio rapido"](#).

Impegni iniziali SaaS

Alcune aziende rendono disponibili i contratti SaaS in anticipo per l'acquisto tramite Marketplace AWS. Con questa opzione, puoi acquistare quantità discrete di licenze o acquisire dati per questi prodotti. Quindi, puoi fatturare questi prodotti, in anticipo, tramite il tuo Account AWS. Ad esempio,

potresti acquistare 10 licenze di accesso utente per un anno oppure acquistare 10 GB di dati importati al giorno per un anno.

Quando effettui l'acquisto, verrai indirizzato al sito Web del prodotto per la configurazione e la configurazione dell'account, a meno che non sia abilitato Quick Launch. I costi di utilizzo vengono quindi visualizzati nel normale rapporto di Account AWS fatturazione.

Note

Per informazioni sull'esperienza di avvio rapido, consulta [the section called “Avvio rapido”](#).

Per sottoscrivere un contratto SaaS

1. Nella pagina dei dettagli del prodotto, scegli Visualizza opzioni di acquisto per avviare la procedura di abbonamento. Puoi scegliere le quantità o le unità che desideri, la durata dell'abbonamento (se sono disponibili più opzioni) e il rinnovo automatico.
2. Dopo aver effettuato le selezioni, scegli Crea contratto.
3. Scegli Configura il tuo account, che ti reindirizza al sito Web dell'azienda. Durante la configurazione dell'account e la verifica del pagamento, nella pagina dei Marketplace AWS dettagli del prodotto vedrai che il contratto è in sospeso.

Note

Alcuni prodotti offrono un'opzione di implementazione Quick Launch, che riduce il tempo e le risorse necessari per configurare, distribuire e avviare il software. Questi prodotti sono identificati mediante un badge Quick Launch. Per ulteriori informazioni, consulta [the section called “Avvio rapido”](#).

Una volta completata la configurazione, nella pagina del prodotto è disponibile un link per configurare l'account. Il software viene visualizzato nella sezione Il tuo software Marketplace quando accedi al tuo Marketplace AWS account. Ora puoi iniziare a utilizzare il software. Se non completi la procedura di configurazione del tuo account, ti verrà richiesto di farlo quando rivisiti quel prodotto su Marketplace AWS

Accedi all'abbonamento al software dal sito Web della società di software utilizzando l'account che hai creato sul loro sito Web. Puoi anche trovare i link ai siti Web per gli abbonamenti software

acquistati nella Marketplace AWS sezione Il tuo software Marketplace dopo aver effettuato l'accesso al tuo Marketplace AWS account.

Versioni di prova gratuite SaaS

Alcuni fornitori offrono prove gratuite per i loro prodotti SaaS a scopo di Marketplace AWS valutazione. Puoi cercare tra i prodotti SaaS Marketplace AWS e filtrare i risultati per mostrare solo quelli con versioni di prova gratuite. I risultati della ricerca indicano quali prodotti offrono prove gratuite. Tutti i prodotti in prova gratuita riportano il badge Prova gratuita accanto al logo del prodotto. Nella pagina di acquisto del prodotto, puoi trovare la durata del periodo di prova gratuito e la quantità di software gratuito inclusa nella versione di prova.

Durante la prova gratuita o dopo la scadenza della prova gratuita, puoi prendere una decisione di acquisto negoziando un'offerta privata o sottoscrivendo un'offerta pubblica. Le versioni di prova gratuite SaaS non si convertono automaticamente in contratti a pagamento. Se non desideri più la prova gratuita, puoi lasciarla scadere.

Puoi visualizzare i tuoi abbonamenti selezionando Gestisci abbonamenti dalla console. Marketplace AWS

Note

Ciascuno Account AWS è idoneo per 1 sola prova gratuita per prodotto.

Abbonamento a un contratto SaaS (offerta di prova gratuita)

Per sottoscrivere un contratto SaaS (offerta di prova gratuita)

1. Accedi alla Marketplace AWS console e scegli Scopri i prodotti dal Marketplace AWS menu.
2. Nel pannello Perfeziona i risultati, vai a Prova gratuita e seleziona Prova gratuita.
3. Per i metodi di consegna, seleziona SaaS.
4. Per il modello di prezzo, seleziona Upfront Commitment per visualizzare tutti i prodotti che offrono prove gratuite. Tutti i prodotti idonei riportano un badge di prova gratuita.
5. Seleziona il prodotto SaaS che desideri.
6. Scegli Prova gratuitamente dalla pagina dei dettagli del prodotto.
7. Per Tipo di offerta, seleziona un'opzione di prova gratuita.

8. Per Acquisto, scegli Crea contratto e poi Accetta contratto.
9. Scegli Configura il tuo account per completare la registrazione e iniziare a utilizzare il software.

Abbonamento a un abbonamento SaaS (offerta di prova gratuita)

Per abbonarsi a un abbonamento SaaS (offerta di prova gratuita)

1. Accedi alla Marketplace AWS console e scegli Scopri i prodotti dal Marketplace AWS menu.
2. Nel pannello Perfeziona i risultati, vai a Prova gratuita e seleziona Prova gratuita.
3. Per i metodi di consegna, seleziona SaaS.
4. Per Modello di prezzo, seleziona Basato sull'utilizzo per visualizzare tutti i prodotti che offrono prove gratuite. Tutti i prodotti idonei riportano un badge di prova gratuita.
5. Seleziona il prodotto SaaS che desideri.
6. Scegli Prova gratuitamente dalla pagina dei dettagli del prodotto.
7. Per Tipo di offerta, seleziona un'opzione di prova gratuita.
8. Per l'acquisto, scegli Abbonati.

Avvio rapido

Quick Launch è un'opzione di Marketplace AWS implementazione disponibile per i prodotti SaaS con Quick Launch abilitato. Riduce il tempo, le risorse e i passaggi necessari per configurare, distribuire e avviare il software. Per i prodotti che offrono questa funzionalità, puoi scegliere di utilizzare Quick Launch o configurare manualmente le tue risorse.

Per trovare, abbonarsi e lanciare un prodotto SaaS utilizzando l'esperienza Quick Launch

1. Vai alla [pagina di Marketplace AWS ricerca](#).
2. Sfoglia Marketplace AWS e trova il prodotto che contiene il software che desideri avviare. I prodotti che offrono l'esperienza Quick Launch hanno il badge Quick Launch nella descrizione del prodotto.

Tip

Per trovare prodotti con l'esperienza Quick Launch abilitata, usa i filtri SaaS e CloudFormation template nel riquadro Perfeziona i risultati.

3. Dopo esserti abbonato al prodotto, vai alla pagina Configura e avvia scegliendo il pulsante Configura il tuo account.
4. Nella pagina di configurazione e avvio del passaggio 1: assicurati di disporre AWS delle autorizzazioni necessarie, assicurati di disporre delle autorizzazioni necessarie per utilizzare l'esperienza di avvio rapido. Contatta l'AWS amministratore per richiedere le autorizzazioni.

Per utilizzare l'esperienza completa di Quick Launch, è necessario disporre delle seguenti autorizzazioni:

- `CreateServiceLinkedRole`— Consente di Marketplace AWS creare il ruolo collegato al `AWSServiceRoleForMarketplaceDeployment` servizio. Questo ruolo collegato al servizio consente di gestire i parametri relativi Marketplace AWS alla distribuzione, archiviati come segreti in, per conto dell'utente. AWS Secrets Manager
 - `DescribeSecrets`— Consente di ottenere informazioni sui Marketplace AWS parametri di distribuzione trasmessi dai venditori.
 - `GetRole`— Consente di Marketplace AWS determinare se il ruolo collegato al servizio è stato creato nell'account.
 - `ListSecrets`— Consente di Marketplace AWS ottenere lo stato dei parametri di distribuzione.
 - `ListRegions`— Consente di Marketplace AWS ottenere Regioni AWS l'iscrizione all'account corrente.
 - `ReplicateSecrets`— Consente di Marketplace AWS avviare la replica dei segreti nella regione selezionata in cui verrà distribuito il software.
5. Per il passaggio 2: accedi a un account fornitore nuovo o esistente, scegli il pulsante Accedi o crea un account. Il sito del venditore si apre in una nuova scheda, in cui puoi accedere o creare un nuovo account. Quando hai finito, torna alla pagina Configura e avvia.
 6. Per la Fase 3: Configurazione del software e AWS dell'integrazione, scegli come configurare il prodotto:
 - `AWS CloudFormation`— Scegliete il pulsante Avvia modello per implementare un CloudFormation modello predefinito per configurare il prodotto. CloudFormation Utilizzatelo per rivedere i parametri del modello e completare eventuali campi aggiuntivi obbligatori. Al termine, torna alla pagina Configura e avvia per avviare il software.
 - `Manuale`: utilizza le istruzioni fornite dal venditore per configurare il software.
 7. Per la Fase 4: Avvia il software, scegli il pulsante Avvia software per avviare il software.

Prodotti Data

È possibile utilizzare Marketplace AWS per trovare e sottoscrivere prodotti di dati disponibili tramite AWS Data Exchange. Per ulteriori informazioni, consulta [Iscrizione a prodotti dati su AWS Data Exchange](#) nella Guida per l'utente di AWS Data Exchange.

Pagamento dei prodotti

All'inizio del mese, ricevi una fattura da Amazon Web Services (AWS) per i tuoi Marketplace AWS addebiti. Per i prodotti software, la fattura include un calcolo della tariffa oraria per il software moltiplicata per il numero di ore di esecuzione di qualsiasi istanza Amazon Machine Image (AMI) con questo software. Riceverai anche una fattura per l'utilizzo di servizi di AWS infrastruttura come Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) e per la larghezza di banda.

Se hai Account AWS sede in Europa, Medio Oriente e Africa (EMEA), esclusi Turchia e Sudafrica, e l'acquisto proviene da un venditore idoneo per l'area EMEA, riceverai una fattura da Amazon Web Services EMEA SARL (). AWS Europe Altrimenti, riceverai una fattura da AWS Inc.

Note

Per gli acquisti contrattuali, la fattura dei canoni di abbonamento viene emessa al momento dell'abbonamento e non nella fattura mensile consolidata. I pagamenti flessibili sui contratti vengono fatturati al momento del pagamento programmato. Per i contratti con componenti di utilizzo (come un pay-as-you-go modello), l'utilizzo viene visualizzato nella fattura mensile consolidata.

Marketplace AWSi prodotti che utilizzano topologie complesse possono comportare costi per cluster di AMI e altri servizi di AWS infrastruttura lanciati dal modello fornito. AWS CloudFormation

Ad esempio, supponiamo di eseguire il software per 720 ore su un tipo di istanza EC2 di piccole dimensioni. La tariffa del venditore per l'utilizzo del software è di 0,12 USD all'ora e gli addebiti EC2 sono di 0,085 USD all'ora. Alla fine del mese, ti verranno fatturati 147,60 USD.

Per ulteriori informazioni sulla sottoscrizione a prodotti di dati, consulta [Subscribing to data products on AWS Data Exchange nella AWS Data Exchange User Guide](#).

Per ulteriori informazioni sul pagamento della AWS fattura, consulta la [Guida per AWS Billing l'utente](#).

Per ulteriori informazioni sulla gestione dei pagamenti in Amazon Web Services EMEA SARL (AWSEurope), consulta [Gestione dei pagamenti AWSEurope nella Guida](#) per l'AWS Billingutente.

Argomenti

- [Ordini di acquisto](#)
- [Informazioni sui rimborsi](#)
- [Annullare l'abbonamento al prodotto](#)
- [Metodi di pagamento](#)
- [Valute supportate](#)
- [Cambiare la valuta preferita](#)
- [Aggiornamento delle istruzioni per le rimesse](#)

Ordini di acquisto

Quando utilizzi gli ordini di acquisto in Marketplace AWS e nella AWS Billing console, ricevi fatture AWS che includono il numero dell'ordine di acquisto definito dal cliente. Questo approccio semplifica l'elaborazione dei pagamenti e l'allocatione dei costi. Nel Marketplace AWS, out-of-cycle le fatture includono gli acquisti che vengono fatturati immediatamente o in base a un pagamento definito programmato in un'offerta privata. In genere, pay-as-you-go gli addebiti appaiono su una fattura di utilizzo Marketplace AWS mensile consolidata.

Utilizzo degli ordini di acquisto per Marketplace AWS le transazioni

Puoi aggiungere un ordine di acquisto al momento della transazione, che verrà applicato a tutte le out-of-cycle fatture successive relative a tale transazione.

I seguenti prodotti supportano gli ordini di acquisto:

- Contratti Software as a Service (SaaS)
- Prodotti di assistenza professionale
- Prodotti server (inclusi istanze AMI, contenitori, AWS CloudFormation modelli e grafici Helm) con un modello di prezzo annuale o contrattuale

Note

Il supporto per gli ordini di acquisto per il modello di prezzo annuale è disponibile solo per le offerte private con un programma di pagamento flessibile.

Gli ordini di acquisto per il modello di prezzo annuale sono supportati solo per le offerte private con un programma di pagamento flessibile. L'ordine di acquisto specificato non si applica alle fatture Marketplace AWS mensili consolidate per pay-as-you-go gli addebiti.

Note

Per utilizzare gli ordini di acquisto in Marketplace AWS, l'account di gestione AWS dell'organizzazione deve abilitare l'AWS Billing integrazione. Questa attività di configurazione unica crea un ruolo collegato al servizio, che consente agli account dell'organizzazione con il permesso di abbonarsi di utilizzare gli ordini di acquisto. Se non abiliti l'integrazione, gli account della tua organizzazione non possono aggiungere un ordine di acquisto durante l'approvvigionamento. Per ulteriori informazioni sull'integrazione, vedere [Creazione di un ruolo collegato ai servizi](#) per Marketplace AWS

Per specificare un ordine di acquisto in Marketplace AWS

1. Trova e preparati ad acquistare un [prodotto supportato](#) da Marketplace AWS.
2. Durante il processo di acquisto, nella pagina Configura l'abbonamento al software (per SaaS), in Ordine di acquisto, scegli Aggiungi il numero dell'ordine di acquisto.
3. Inserisci il numero dell'ordine di acquisto nel campo Numero dell'ordine di acquisto.

Il numero dell'ordine di acquisto è il numero o il testo che utilizzi per tracciare l'ordine di acquisto nel tuo sistema. Di solito viene emesso da un sistema o da un processo interno. Può contenere fino a 200 caratteri.

Per informazioni dettagliate su un ordine di acquisto, inclusi gli ordini di acquisto forniti durante Marketplace AWS le transazioni, utilizza la [dashboard degli ordini di acquisto nella AWS Billing console](#).

Utilizzo degli ordini di acquisto con utilizzo generalizzato

Per separare gli Marketplace AWS addebiti dagli altri ordini di acquisto, puoi creare un ordine di acquisto con una voce di utilizzo Marketplace AWS generica nella AWS Billing console. Marketplace AWS le transazioni con fattura includeranno l'ordine di acquisto per uso generale specificato se determinati criteri e parametri corrispondono (ad esempio, le entità di fatturazione). Un'eccezione sono le out-of-cycle fatture che hanno specificato un ordine di acquisto relativo a una Marketplace

AWS transazione. Per ulteriori informazioni, consulta [la sezione Gestione degli ordini di acquisto](#) nella Guida per l'utente di AWS Billing and Cost Management.

Risoluzione dei problemi relativi agli ordini

Le informazioni contenute nella tabella seguente possono aiutarti a risolvere i problemi relativi agli ordini di acquisto o a capire cosa succede in diversi scenari.

Scenario	Informazioni
Autorizzazioni insufficienti	La nota viene visualizzata accanto al campo di immissione dell'ordine di acquisto se non disponi dell'autorizzazione <code>aws-marketplace:Subscribe</code> per la sottoscrizione. L'account di gestione deve inoltre abilitare l'AWS Billing integrazione. Per informazioni sull'abilitazione dell'integrazione, vedere Creazione di un ruolo collegato ai servizi per Marketplace AWS
L'ordine di acquisto non esiste	Marketplace AWS crea un nuovo ordine di acquisto per te. Il nuovo ordine di acquisto contiene informazioni predefinite, senza informazioni di contatto.
Notifiche relative agli ordini di acquisto mancanti	Gli ordini di acquisto senza informazioni di contatto (inclusi gli ordini di acquisto creati da Marketplace AWS) non ricevono notifiche e-mail. Puoi aggiungere informazioni di contatto a un ordine di acquisto nella dashboard Ordini di acquisto nella console di fatturazione e gestione dei costi .
È stato aggiunto un numero di ordine di acquisto errato	Se inserisci un numero dell'ordine di acquisto errato e devi aggiornarlo, contattaci AWS Support per aggiornare il numero dell'ordine di acquisto.

Scenario	Informazioni
L'account di iscrizione viene trasferito a un'altra organizzazione	Affinché gli ordini di acquisto funzionino nella nuova organizzazione, l'integrazione deve essere completata nella nuova organizzazione. Se l'integrazione è stata completata e il supporto per gli ordini di acquisto funziona nella nuova organizzazione, quando l'account di sottoscrizione passa da un'organizzazione all'altra, le nuove fatture mostrano il numero dell'ordine di acquisto nella nuova organizzazione (e viene creato un nuovo ordine di acquisto, se necessario).
Opzione ordine di acquisto non disponibile al momento del check-out	L'AWS Billing integrazione è disponibile solo per i contratti SaaS, i prodotti di servizi professionali e i prodotti server con prezzi contrattuali e i prodotti server con prezzi annuali per le offerte private con un programma di pagamento flessibile.
Contratti con pay-as-you-go	La fattura del contratto riporta il numero dell'ordine di acquisto, ma la fattura di consumo (pay as you go) non mostra il numero dell'ordine di acquisto. Il pay-as-you-go modello non supporta l'aggiunta di numeri di ordine di acquisto. Valuta la possibilità di aggiungere un ordine di acquisto con una voce di utilizzo Marketplace AWS generica nella AWS Billing console.

Scenario	Informazioni
Ordine di acquisto sospeso	Quando viene fornito un numero di ordine di acquisto e l'ordine di acquisto viene contrassegnato come sospeso nella dashboard Ordini di acquisto nella console di fatturazione e gestione dei costi, la nuova voce viene aggiunta all'ordine di acquisto, ma la fattura non include l'ordine di acquisto. L'amministratore della fatturazione per le Account AWS esige di rendere attivo l'ordine di acquisto e il contatto AWS Support per rigenerare la fattura con l'ordine di acquisto attivo.
Ordine di acquisto scaduto	Quando viene fornito un numero di ordine di acquisto e l'ordine di acquisto è scaduto, viene creata la nuova voce e l'ordine di acquisto viene contrassegnato come attivo. La data di fine dell'articolo viene utilizzata come data di scadenza del nuovo ordine di acquisto.
Monitoraggio del saldo	Il monitoraggio del saldo non è abilitato Marketplace AWS per le voci.
Integrazione del sistema di approvvigionamento	L'ordine di acquisto fornito da un sistema di approvvigionamento integrato è riportato sulle fatture.
Pianificazione flessibile dei pagamenti - acquisto iniziale	Un contratto con date di fatturazione specifiche e (programma di pagamento flessibile) genera una voce iniziale nell'ordine di acquisto per zero dollari. Per ogni fattura vengono create voci aggiuntive con prezzi applicabili.

Scenario	Informazioni
Pianificazione dei pagamenti flessibile: ordini di acquisto multipli	Se hai bisogno di pagamenti individuali per un piano di pagamento flessibile da visualizzare con diversi ordini di acquisto, contattaci AWS Support per modificare il numero dell'ordine di acquisto nelle fatture future.

Informazioni sui rimborsi

I clienti possono richiedere diversi tipi di rimborsi per Marketplace AWS i prodotti. Per Marketplace AWS i prodotti venduti da AWS, consulta la pagina sulla politica di rimborso e quindi invia il modulo di assistenza di contatto utilizzando il AWS Support Center Console. Se il prodotto è venduto da una terza parte, consulta le politiche di rimborso nella pagina dei dettagli del prodotto. Le spese software per Marketplace AWS gli abbonamenti vengono pagate al venditore del prodotto e i rimborsi devono essere richiesti direttamente al venditore. Ogni Marketplace AWS venditore è tenuto a includere una politica di rimborso sulla propria Marketplace AWS pagina.

Per ulteriori informazioni sui rimborsi relativi agli Marketplace AWS acquisti, consulta gli argomenti seguenti nella Guida per il Marketplace AWS venditore:

- [Refunds](#) (Rimborsi)
- [Prezzi dei prodotti](#)

Note

Per tutti i rimborsi relativi alle offerte private, contatta il venditore.

Annullare l'abbonamento al prodotto

Puoi annullare l'abbonamento al prodotto o il rinnovo automatico in Marketplace AWS. I passaggi seguenti forniscono istruzioni per i prodotti Software as a Service (SaaS), machine learning (ML) e Amazon Machine Image (AMI) inclusi Marketplace AWS.

Argomenti

- [Annullare l'abbonamento SaaS](#)
- [Annullare l'abbonamento al machine learning](#)
- [Annullare l'abbonamento AMI](#)
- [Annulla il rinnovo automatico dell'abbonamento al contratto SaaS](#)

Annullare l'abbonamento SaaS

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Vai alla pagina [Gestisci abbonamenti](#).
3. Per il metodo di consegna, scegli SaaS dall'elenco a discesa.
4. Seleziona l'abbonamento per il prodotto per il prodotto che si desidera annullare l'abbonamento per il prodotto che si desidera annullare l'abbonamento per
5. Scegliere Cancel subscription (Annulla sottoscrizione).

Annullare l'abbonamento al machine learning

Prima di annullare l'abbonamento al machine learning, esegui le seguenti azioni:

- Per gli algoritmi ML: accedi AWS Management Console e apri la SageMaker console [Amazon](#). Interrompi qualsiasi processo di addestramento in corso per il tuo algoritmo. Se hai creato un pacchetto modello dal tuo algoritmo, non puoi avviare un endpoint in tempo reale o creare un processo di inferenza in batch dopo l'annullamento dell'abbonamento al machine learning.
- Per pacchetti di modelli ML o modelli creati dai tuoi algoritmi, accedi AWS Management Console e apri la SageMaker console [Amazon](#). Interrompi tutti gli endpoint in esecuzione in tempo reale per i tuoi modelli o interrompi qualsiasi processo di inferenza batch in esecuzione.

Note

I job e gli endpoint esistenti che non vengono terminati continueranno a essere eseguiti e verranno fatturati fino alla loro conclusione.

Per annullare un abbonamento di machine learning

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).

2. Vai alla pagina [I miei abbonamenti](#).
3. Seleziona l'abbonamento per il prodotto per il prodotto che si desidera annullare l'abbonamento per il prodotto che si desidera annullare l'abbonamento per
4. Scegliere Cancel subscription (Annulla sottoscrizione). Dopo aver annullato l'abbonamento, non puoi avviare l'algoritmo o il modello.

Annullare l'abbonamento AMI

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Vai alla pagina [Gestisci abbonamenti](#).
3. Per il metodo di consegna, scegli Amazon Machine Image dall'elenco a discesa.
4. Seleziona l'abbonamento per il prodotto per il prodotto che si desidera annullare l'abbonamento per il prodotto che si desidera annullare l'abbonamento per
5. Dall'elenco a discesa Azioni, scegli Annulla abbonamento.
6. Leggi le informazioni fornite nella sezione Riconosci che le istanze in esecuzione vengono addebitate sul tuo account e seleziona la casella di controllo. Scegliere Yes, cancel subscription (Sì, annulla sottoscrizione).
7. ApriAWS il riquadro
8. Termina l'istanze in esecuzione nella console Amazon EC2. Se sono in esecuzione più istanze, è necessario terminarle tutte. Inoltre, è necessario eliminareAWS CloudFormation gli stack, se applicabile.
9. Torna alla scheda Gestisci abbonamenti e scegli Sì, Annulla abbonamento. Dopo aver annullato l'abbonamento, perdi l'accesso al software e non ti verrà più addebitato alcun costo.

Annulla il rinnovo automatico dell'abbonamento al contratto SaaS

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Vai alla pagina dei dettagli del prodotto.
3. Scegli Continua per accedere alla pagina degli ordini.
4. Scegli la scheda Modifica rinnovo, quindi scegli Annulla rinnovo.

Metodi di pagamento

Quando hai creato il tuo account per la prima volta Account AWS, hai impostato il metodo di pagamento per quell'account. Puoi gestire i tuoi metodi di pagamento nella [console di fatturazione e gestione dei costi di AWS](#). Per istruzioni, consulta [Gestione dei pagamenti](#) nella Guida per l'AWS Billingutente.

Errori di pagamento

Se si verifica un errore durante l'elaborazione del pagamento tramite il tuo account pagatore, aggiorna il metodo di pagamento e riprova. Gli errori possono verificarsi perché:

- Il metodo di pagamento è mancante, non valido o non supportato.
- Il pagamento è stato rifiutato.
- Il tuo account Amazon Internet Services Private Limited (AISPL) limita l'uso di carte di debito o di credito per i nuovi acquisti con un modello di prezzo contrattuale. Se disponi di un account AISPL, contatta il [Servizio clienti AWS](#) per aggiornare il metodo di pagamento predefinito. Per maggiori dettagli, consulta [Restrizione agli acquisti con carta di credito e di debito per i clienti AISPL che utilizzano](#) il sito Web del Marketplace AWS Marketplace AWS blog.
- La tua offerta privata include un piano di pagamento. Tuttavia, il tuo metodo di pagamento predefinito non è impostato sui termini di fatturazione.

I metodi di pagamento aggiornati possono richiedere fino a 7 giorni per diventare disponibili per i nuovi acquisti. Per assistenza con la risoluzione dei problemi, contatta [AWS Support](#).

Valute supportate

Gli elenchi seguenti includono tutte le valute supportate esistenti per AWS Amazon Web Services EMEA SARL.

Note

La rupia indiana (INR) non è una valuta supportata perché Amazon Internet Services Private Limited (AISPL) non è attualmente supportata su Marketplace AWS. Per ulteriori informazioni, vedi [Quali sono le differenze tra account Account AWS e account AISPL](#).

Le valute supportate per Amazon Web Services sono le seguenti:

- Dollaro australiano (AUD)
- Sterlina britannica (GBP)
- Dollaro canadese (CAD)
- Corona danese (DKK)
- Euro (EUR)
- Dollaro di Hong Kong (HKD)
- Yen giapponese (JPY)
- Dollaro neozelandese (NZD)
- Corona norvegese (NOK)
- Dollaro di Singapore (SGD)
- Rand sudafricano (ZAR)
- Corona svedese (SEK)
- Franco svizzero (CHF)
- Dollaro USA (USD)

Le valute supportate per Amazon Web Services EMEA SARL sono le seguenti:

- Sterlina britannica (GBP)
- Corona danese (DKK)
- Euro (EUR)
- Corona norvegese (NOK)
- Rand sudafricano (ZAR)
- Corona svedese (SEK)
- Franco svizzero (CHF)
- Dollaro USA (USD)

Cambiare la valuta preferita

Marketplace AWS I tuoi acquisti vengono visualizzati nella valuta che hai specificato per il tuo Account AWS. Puoi modificare la valuta preferita per il tuo account nella [AWS Billing and Cost](#)

[Managementconsole](#). Per istruzioni, consulta [Modifica della valuta utilizzata per pagare la fattura](#) nella Guida per l'AWS Billingutente.

Note

La modifica della valuta preferita modifica le istruzioni di rimessa. [Per visualizzare le istruzioni di pagamento aggiornate, consulta la Marketplace AWS fattura o visualizza la pagina Impostazioni account nella console. AWS Billing and Cost Management](#)

Aggiornamento delle istruzioni per le rimesse

I clienti con Account AWS sede in Europa, Medio Oriente e Africa (EMEA), esclusi Turchia e Sudafrica, che hanno acquistato prodotti software da venditori idonei all'area EMEA ricevono una fattura da Amazon Web Services EMEA SARL. [Le fatture di Amazon Web Services EMEA SARL \(AWS Europe\) hanno istruzioni di pagamento diverse da quelle di AWS, Inc. Puoi trovare informazioni sulle rimesse nelle tue fatture dopo aver effettuato l'accesso alla console. AWS Billing and Cost Management](#) I conti bancari elencati nella sezione relativa alle informazioni di rimessa della fattura sono diversi dagli acquisti di servizi tramite Amazon Web Cloud AWS Services EMEA SARL. Amazon Web Services EMEA SARL utilizza Amazon Payments Europe, S.C.A., un istituto di moneta elettronica autorizzato in Lussemburgo, come processore di pagamento per le fatture. Marketplace AWS Tutte le fatture devono essere saldate per intero. Tutti i pagamenti che non coprono l'intero importo della fattura verranno rimborsati sul tuo conto bancario.

La tabella seguente descrive i tipi di transazione, l'entità che effettua la transazione e le istruzioni di rimessa corrispondenti (Nome del conto elencato in Dettagli del trasferimento elettronico di fondi nella fattura).

Tipo di transazione	Entità che effettua transazioni	Istruzioni per le rimesse
Cloud AWS acquisti di servizi	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
Marketplace AWS Venditore idoneo	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
Venditore non idoneo Marketplace AWS	AWS Inc.	AWS

<Per richiedere una lettera bancaria contenente le istruzioni per il pagamento,

Per ulteriori informazioni su come modificare la tua preferenza di valuta con una valuta supportata, consulta [Modifica della valuta utilizzata per pagare la fattura](#) nella Guida per l'AWS Billingutente.

Amazon Web Services EMEA SARL accetta pagamenti tramite trasferimento elettronico di fondiMasterCard, tramite carte di credito VISA e American Express. Le carte di credito Diner's Club o Discover non sono accettate.

Per ulteriori informazioni, consulta la [Guida fiscale degli Marketplace AWS acquirenti](#).

Etichettatura per l'allocazione dei costi

Marketplace AWS supporta l'assegnazione di tag per l'allocazione dei costi per i prodotti software acquistati. Puoi utilizzare i tag di allocazione dei costi attivati per identificare e tenere traccia dell'utilizzo Marketplace AWS delle risorse tramite AWS Cost Explorer report su AWS costi e utilizzo, AWS budget o altri strumenti di analisi dei costi cloud. Per semplificare la allocazione e il monitoraggio Marketplace AWS dei costi, è possibile utilizzare i tag per allocazione dei costi per organizzare i costi per organizzare i costi nel report.

I tag di allocazione dei costi Marketplace AWS provengono dalle due fonti seguenti:

- I costi associati a un'istanza Amazon Machine Image (AMI) associati a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) con tag ereditano gli stessi tag. Puoi attivare questi tag come tag con allocazione dei costi nella AWS Billing and Cost Management console di un account. Per ulteriori informazioni sull'utilizzo dei tag di allocazione dei costi con i prodotti AMI, consulta [Etichettatura dell'allocazione dei costi nei prodotti AMI](#).
- I prodotti AMI, container e software as a service (SaaS) possono avere tag forniti dal fornitore. Ad esempio, un prodotto SaaS che fattura in base al numero di utenti potrebbe utilizzare un tag per identificare l'utilizzo per reparto. Per ulteriori informazioni sull'utilizzo di questi tag, consulta [Etichette misurate dal fornitore](#).

La allocazione dei costi tiene traccia solo dei costi a partire dal momento in cui i tag sono stati attivati nella console di allocazione dei costi, a partire dal momento in cui i tag sono stati attivati nella console di allocazione Billing and Cost Management. Solo Account AWS i proprietari, i proprietari degli account di AWS Organizations gestione e gli utenti con le autorizzazioni appropriate possono accedere alla console di Billing and Cost Management di un account. Indipendentemente dal fatto che utilizzi i tag di allocazione dei costi, l'importo fatturato non cambia. L'uso o meno dei tag di allocazione dei costi non ha alcun impatto sulla funzionalità dei prodotti Marketplace AWS software.

Per gli abbonamenti di venditori idonei all'area EMEA, il rapporto costi e utilizzo include una colonna per la parte AWS contraente (Amazon Web Services EMEA SARL).

Etichette misurate dal fornitore

Marketplace AWS i prodotti con misurazione dei fornitori (inclusi prodotti AMI, container e SaaS) potrebbero avere tag forniti dal fornitore del software come servizio aggiuntivo per i propri clienti.

Questi tag sono tag di allocazione dei costi che consentono di comprendere l'utilizzo Marketplace AWS delle risorse in base alle metriche fornite dal fornitore. Puoi utilizzare questi tag per identificare e monitorare l'utilizzo Marketplace AWS delle risorse tramite AWS Cost Explorer Service, AWS Cost and Usage Report Budget AWS, o altri strumenti di analisi dei costi del cloud.

I tag vengono visualizzati nella AWS Billing console dopo aver iniziato a utilizzare il Marketplace AWS prodotto e il fornitore invia i record di misurazione a Marketplace AWS. Se utilizzi un prodotto sulla base di un impegno iniziale in un contratto, non riceverai la misurazione dell'utilizzo del prodotto. Di conseguenza, non avrai i tag misurati dal fornitore nella tua AWS Billing console. Se gestisci un account collegato, devi disporre sia delle autorizzazioni che ViewBilling delle autorizzazioni per visualizzare e attivare i tag AWS Billing. ModifyBilling Per ulteriori informazioni, consulta le [policy relative alle azioni di fatturazione](#) di AWS nella Guida per l'utente di fatturazione AWS.

Note

L'attivazione di tag basati sui parametri del fornitore potrebbe aumentare le dimensioni del rapporto sui costi e sull'utilizzo. Il report sui costi e sull'utilizzo è archiviato in Amazon S3. Pertanto, anche i costi di Amazon S3 potrebbero aumentare.

Per attivare i tag basati sui parametri del fornitore per tutti i Marketplace AWS prodotti idonei

1. Accedere alla AWS Management Console e aprire la [console AWS Billing](#). Quindi scegli i tag di allocazione dei costi dal riquadro di navigazione a sinistra.
2. Scegli la scheda dei tag AWS generati da.
3. Cerca per `aws:marketplace:isv`: trovare i tag per tutti i prodotti che supportano l'etichettatura basata sui parametri del fornitore.
4. Seleziona le caselle di controllo per tutti i tag, quindi scegli Attiva. I tag misurati dal fornitore entreranno in vigore entro 24 ore.

Argomenti correlati

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Uso dei tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing.
- [Attivazione dei tag di allocazione dei costi generati da AWS](#) nella Guida per l'AWS Billing utente

Mercati privati

Un marketplace privato controlla i prodotti che gli utenti del tuo Account AWS sito, come gli utenti aziendali e i team di progettazione, possono acquistare. Marketplace AWS Si basa su e consente agli amministratori di Marketplace AWS creare e personalizzare cataloghi digitali curati di fornitori di software indipendenti (ISV) approvati e prodotti conformi alle loro politiche interne. Gli utenti Account AWS possono trovare, acquistare e distribuire prodotti approvati dal vostro marketplace privato e garantire che tutti i prodotti disponibili siano conformi alle politiche e agli standard della vostra organizzazione.

Un marketplace privato offre un ampio catalogo di prodotti disponibili in Marketplace AWS, oltre a un controllo approfondito di tali prodotti. Con [AWS Organizations](#), è possibile centralizzare la gestione di tutti gli account, raggrupparli in unità organizzative (OU) e applicare politiche di accesso diverse a ciascuna unità organizzativa. Puoi creare più esperienze di marketplace private associate all'intera organizzazione, a una o più unità organizzative o a uno o più account dell'organizzazione, ognuna con il proprio set di prodotti approvati. AWS Gli amministratori possono anche applicare il marchio aziendale a ogni esperienza di marketplace privato con il logo, i messaggi e lo schema di colori dell'azienda o del team.

Questa sezione descrive l'utilizzo del marketplace privato come acquirente. Per informazioni sulla gestione dei marketplace privati come amministratore, consulta [Creazione e gestione di un marketplace privato](#).

Note

- Puoi aggiungere prodotti privati che sono stati condivisi con te (tramite un'[offerta privata](#)) a un marketplace privato. Per ulteriori informazioni, consulta [Abbonamento a un prodotto privato in un marketplace privato](#).
- In un marketplace privato, i clienti hanno automaticamente diritto a tutti i prodotti i cui EULA sono regolati dal Contratto con il AWS cliente o da un altro accordo AWS che disciplina l'uso di. Servizi AWS I clienti hanno già diritto a questi prodotti per impostazione predefinita; pertanto, non sono inclusi nell'elenco dei prodotti che hai approvato nel tuo marketplace privato. I clienti possono utilizzare Service Catalog per gestire l'implementazione di questi prodotti.

Visualizzazione delle pagine dei dettagli del prodotto

Gli utenti possono abbonarsi solo ai prodotti che hai consentito nel marketplace privato che gestisce l'account. Possono sfogliare e visualizzare la pagina dei dettagli di qualsiasi prodotto, ma l'abbonamento è abilitato solo per i prodotti che hai aggiunto al tuo marketplace privato. Se un prodotto non è attualmente presente nel tuo marketplace privato, l'utente visualizza un banner rosso nella parte superiore della pagina, che indica che il prodotto non è approvato per l'approvvigionamento. Marketplace AWS

Se le richieste software sono abilitate, gli utenti possono scegliere Crea richiesta nella pagina dei dettagli del prodotto. Quando gli utenti scelgono Crea richiesta, inviano una richiesta all'amministratore per rendere il prodotto disponibile sul tuo marketplace privato. Per ulteriori informazioni sull'utilizzo di questa caratteristica, consulta [Gestione delle richieste degli utenti](#).

Abbonamento a un prodotto in un marketplace privato

Per abbonarti a un prodotto nel tuo marketplace privato come utente, vai alla pagina dei dettagli del prodotto e scegli Continua. Questo ti reindirizza alla pagina di abbonamento del prodotto. Nella pagina di abbonamento, puoi effettuare le selezioni di configurazione e quindi scegliere Abbonati.

Se il prodotto non è approvato nel tuo marketplace privato, Subscribe non è disponibile. Un banner rosso nella parte superiore della pagina indica che il prodotto non è attualmente approvato per l'approvvigionamento. Se le richieste software sono abilitate, puoi scegliere Crea richiesta per inviare una richiesta all'amministratore per richiedere che il prodotto venga aggiunto al tuo marketplace privato.

Abbonamento a un prodotto privato in un marketplace privato

Alcuni prodotti non sono disponibili pubblicamente per la navigazione. Marketplace AWS Questi prodotti possono essere visualizzati solo quando ti viene offerta un'offerta privata dal venditore. Tuttavia, puoi abbonarti solo se l'amministratore del marketplace privato aggiunge prima il prodotto al tuo marketplace privato. Per questo motivo, l'offerta privata deve essere estesa sia al tuo Account AWS account che all'account che include l'amministratore del marketplace privato della tua organizzazione. Dopo che l'offerta privata è stata estesa sia all'utente che all'amministratore, l'amministratore del marketplace privato può aggiungere il prodotto al tuo marketplace privato. Dopo l'approvazione del prodotto, puoi abbonarti al prodotto come qualsiasi altra offerta privata.

Richiedere l'aggiunta di un prodotto al tuo marketplace privato

Come utente, puoi richiedere all'amministratore di aggiungere un prodotto che non si trova nel tuo marketplace privato. Per effettuare una richiesta, accedi alla pagina dei dettagli del prodotto, scegli Crea richiesta, inserisci una richiesta all'amministratore affinché il prodotto venga aggiunto al tuo marketplace privato, quindi invia la richiesta. Per monitorare lo stato della tua richiesta, nel menu a discesa a sinistra, scegli Le tue richieste sul Marketplace privato.

Creazione e gestione di un marketplace privato

Per creare e gestire un marketplace privato, devi accedere all'account di gestione o all'account amministratore delegato del marketplace privato. È inoltre necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) previste nella `AWSPrivateMarketplaceAdminFullAccess` policy IAM. Per ulteriori informazioni sull'applicazione di questa politica a utenti, gruppi e ruoli, consulta [the section called “Creazione di un amministratore del marketplace privato”](#).

Note

Se attualmente sei un cliente di Private Marketplace e non AWS Organizations disponi dell'integrazione per Private Marketplace, puoi creare e gestire un marketplace privato da qualsiasi account della tua organizzazione che disponga della policy `AWSPrivateMarketplaceAdminFullAccess` IAM.

Questa sezione include le attività che puoi completare come amministratore del marketplace privato tramite il Marketplace AWS sito web. Puoi anche gestire i marketplace privati utilizzando AWS Marketplace Catalog API Per ulteriori informazioni, consulta [Lavorare con un marketplace privato](#) nella Guida AWS Marketplace Catalog API di riferimento.

Guida introduttiva a Private Marketplace

Per iniziare a usare Private Marketplace, assicurati di aver effettuato l'accesso al tuo account di AWS gestione, accedi a [Private Marketplace](#) e abilita i seguenti prerequisiti:

- **Accesso affidabile:** devi abilitare l'accesso affidabile per AWS Organizations, che consente all'account di gestione di un'organizzazione di fornire o revocare l'accesso ai propri AWS Organizations dati per un servizio. AWS Consentire l'accesso affidabile è fondamentale per

consentire a Private Marketplace di integrarsi con Private Marketplace AWS Organizations e designare Private Marketplace come servizio affidabile all'interno dell'organizzazione.

- Ruolo collegato al servizio: devi abilitare il ruolo collegato ai servizi del marketplace privato, che risiede nell'account di gestione e include tutte le autorizzazioni richieste da Private Marketplace per descrivere AWS Organizations e aggiornare le risorse del marketplace privato per tuo conto. Per ulteriori informazioni sul ruolo collegato al servizio, consulta [Utilizzo dei ruoli per configurare Private Marketplace](#) in Marketplace AWS

Note

Gli attuali clienti del Marketplace privato possono abilitare le impostazioni per il tuo marketplace privato accedendo alla pagina dell'amministratore del Marketplace privato e selezionando Impostazioni. Consentendo l'accesso affidabile AWS Organizations e creando un ruolo collegato ai servizi, puoi utilizzare funzionalità, come l'associazione delle unità organizzative alle esperienze di marketplace private e la registrazione di un amministratore delegato. Se abilitati, solo l'account di gestione e l'account amministratore delegato possono creare e gestire esperienze di marketplace, con le risorse esistenti trasferite all'account di gestione e condivise solo con l'amministratore delegato. La disabilitazione dell'accesso affidabile eliminerà la governance del marketplace privato per l'organizzazione. Non ci sono gruppi di account visualizzati nel tuo marketplace privato. Per visualizzare la governance della tua organizzazione a diversi livelli, utilizza la pagina Struttura dell'organizzazione. Per domande o assistenza, [contattaci](#).

Gestione del mercato privato

Puoi gestire il tuo marketplace privato dalla pagina dell'amministratore di Private Marketplace in Impostazioni nel riquadro a sinistra. L'amministratore dell'account di gestione e gli amministratori delegati possono utilizzare questa pagina per visualizzare i dettagli del marketplace privato, inclusi il marketplace privato predefinito e il numero di esperienze live.

Gli amministratori degli account di gestione possono utilizzare questa pagina anche per gestire le seguenti impostazioni.

Amministratori delegati

L'amministratore dell'account di gestione può delegare le autorizzazioni amministrative del marketplace privato a un account membro designato noto come amministratore delegato. Per registrare un account come amministratore delegato per il marketplace privato, l'amministratore dell'account di gestione deve assicurarsi che l'accesso affidabile e il ruolo collegato al servizio siano abilitati, scegliere Registra un nuovo amministratore, fornire il numero di account a 12 cifre AWS e scegliere Invia.

Gli account di gestione e gli account amministratore delegato possono eseguire attività amministrative del marketplace privato, come la creazione di esperienze, l'aggiornamento delle impostazioni di branding, l'associazione o la dissociazione dei segmenti di pubblico, l'aggiunta o la rimozione di prodotti e l'approvazione o il rifiuto delle richieste in sospeso.

Accesso affidabile e ruolo collegato al servizio

L'amministratore dell'account di gestione può abilitare le seguenti funzionalità per il tuo marketplace privato.

Note

Gli attuali clienti del Marketplace privato possono abilitare le impostazioni per il tuo marketplace privato accedendo alla pagina dell'amministratore del Marketplace privato e selezionando Impostazioni. Consentendo l'accesso affidabile AWS Organizations e creando un ruolo collegato ai servizi, puoi utilizzare funzionalità, come l'associazione delle unità organizzative alle esperienze di marketplace private e la registrazione di un amministratore delegato. Se abilitati, solo l'account di gestione e l'account amministratore delegato possono creare e gestire esperienze di marketplace, con le risorse esistenti trasferite all'account di gestione e condivise solo con l'amministratore delegato. La disabilitazione dell'accesso affidabile eliminerà la governance del marketplace privato per l'organizzazione. Non ci sono gruppi di account visualizzati nel tuo marketplace privato. Per visualizzare la governance della tua organizzazione a diversi livelli, utilizza la pagina Struttura dell'organizzazione. Per domande o assistenza, [contattaci](#).

- **Accesso affidabile:** è necessario abilitare l'accesso affidabile per AWS Organizations, che consente all'account di gestione di un'organizzazione di fornire o revocare l'accesso ai propri AWS Organizations dati per un AWS servizio. Consentire l'accesso affidabile è fondamentale

per consentire a Private Marketplace di integrarsi con Private Marketplace AWS Organizations e designare Private Marketplace come servizio affidabile all'interno dell'organizzazione.

- Ruolo collegato al servizio: devi abilitare il ruolo collegato ai servizi del marketplace privato, che risiede nell'account di gestione e include tutte le autorizzazioni richieste da Private Marketplace per descrivere AWS Organizations e aggiornare le risorse del marketplace privato per tuo conto. Per ulteriori informazioni sul ruolo collegato al servizio, consulta [Utilizzo dei ruoli per configurare Private Marketplace](#) in Marketplace AWS

Creazione di un'esperienza di marketplace privata

Il tuo marketplace privato è composto da una o più esperienze di marketplace private. Un'esperienza può essere associata all'intera organizzazione, a una o più unità organizzative o a uno o più account dell'organizzazione. Se Account AWS non sei membro di un'organizzazione, hai un'esperienza di marketplace privata associata a un account. Per creare il tuo marketplace privato, accedi a [Private Marketplace](#), seleziona la pagina Esperienze a sinistra e scegli Crea esperienza.

Note

Per utilizzare Private Marketplace con AWS Organizations, devi abilitare tutte le funzionalità per l'organizzazione. Per ulteriori informazioni, consulta la sezione [Abilitazione di tutte le caratteristiche nell'organizzazione](#) nella Guida per l'utente di AWS Organizations. Se Account AWS non sei membro di un'organizzazione, non sono necessari passaggi preliminari per utilizzare Private Marketplace.

La tua esperienza di marketplace privato viene creata senza prodotti approvati, senza elementi di branding e non è associata a nessun account all'interno dell'organizzazione. Per impostazione predefinita, non è attivo. I seguenti argomenti descrivono come utilizzare la tua esperienza di marketplace privata.

Aggiungere prodotti alla tua esperienza di marketplace privato

Per aggiungere prodotti a un'esperienza di marketplace privata

1. Dalla pagina dell'amministratore di Private Marketplace, seleziona Esperienze nel riquadro di navigazione a sinistra. Quindi, nella scheda Prodotti, scegli Tutti i prodotti AWS Marketplace. Puoi cercare per nome del prodotto o nome del venditore.

2. Seleziona la casella di controllo accanto a ciascun prodotto da aggiungere al tuo marketplace privato, quindi scegli Aggiungi a Private Marketplace.

Note

Puoi anche aggiungere un prodotto direttamente dalla pagina dei dettagli del prodotto scegliendo il pulsante Aggiungi a Private Marketplace sul banner rosso. Se il banner rosso non si trova nella pagina dei dettagli del prodotto, il prodotto è già presente nel tuo marketplace privato.

Puoi anche aggiungere più prodotti a più esperienze contemporaneamente selezionando Aggiungi/rimuovi prodotti in blocco dal riquadro di navigazione a sinistra.

Verifica dei prodotti nella tua esperienza di marketplace privata

Per verificare che un prodotto sia approvato nell'ambito della tua esperienza di marketplace privata

1. Dalla pagina dell'amministratore di Private Marketplace, seleziona Esperienze nel riquadro di navigazione a sinistra.
2. Scegli Prodotti approvati. Tutti i prodotti approvati vengono visualizzati nell'elenco approvati.

Note

Se utilizzi un account associato all'esperienza che stai modificando e l'esperienza è abilitata, puoi anche visualizzare i prodotti direttamente nella Marketplace AWS console (<https://console.aws.amazon.com/marketplace>). Tutti i prodotti presenti nei risultati di ricerca mostrano un badge approvato per l'approvvigionamento, se fanno parte del tuo marketplace privato.

Personalizzazione della tua esperienza sul marketplace privato

Le esperienze sono sottoinsiemi di prodotti e marchi associati che possono avere uno o più segmenti di pubblico associati. Un'unica esperienza di marketplace privato può governare l'intera organizzazione se l'esperienza è associata all'organizzazione o gestire uno o più account o unità organizzative dell'organizzazione.

Puoi gestire le impostazioni della tua esperienza dalla pagina dell'amministratore di Private Marketplace sotto Esperienze nel riquadro a sinistra. Usa questa pagina per visualizzare e gestire tutte le tue esperienze attive e archiviate e creare nuove esperienze per il tuo marketplace privato. Per ogni esperienza, puoi aggiungere un logo, aggiungere un titolo e personalizzare l'interfaccia utente per utilizzare lo schema di colori della tua organizzazione.

Gestire il pubblico

Un pubblico è un'organizzazione o un gruppo di unità organizzative (OU) o account che puoi associare a un'esperienza di marketplace privata. Puoi creare un pubblico dalla pagina dell'amministratore di Private Marketplace sotto Esperienze nel riquadro a sinistra.

Puoi associare uno o più segmenti di pubblico a un'esperienza. L'associazione o la dissociazione di un gruppo di destinatari può modificare l'esperienza di gestione delle unità organizzative e degli account secondari. Utilizza la pagina Struttura organizzativa per visualizzare gli account e le unità organizzative interessati dall'associazione. Se disabiliti l'accesso affidabile, i tuoi destinatari verranno dissociati e tutta la governance verrà rimossa.

Note

Puoi visualizzare la tua AWS Organizations gerarchia e gestire la governance della tua organizzazione da un marketplace privato. Per gestire il marketplace privato a livello di unità organizzativa e registrare gli amministratori delegati, abilita l'accesso affidabile e il ruolo collegato al servizio dalla pagina Impostazioni. [Per domande o assistenza, contattaci.](#)

Configurazione del tuo marketplace privato

Dopo aver soddisfatto l'elenco dei prodotti dell'esperienza, le impostazioni di branding del marketplace e i gruppi di account associati, puoi rendere attivo il tuo marketplace privato. Dalla pagina dell'amministratore di AWS Private Marketplace, seleziona Esperienza nel riquadro di navigazione a sinistra, quindi seleziona l'esperienza che desideri abilitare. Nella scheda Impostazioni, puoi modificare lo stato del marketplace privato tra Live (abilitato) e Non live (disabilitato).

Puoi anche scegliere di consentire agli utenti di inviare richieste software con le richieste software. Se le richieste software sono attivate (abilite), gli utenti finali possono scegliere Crea richiesta nella pagina dei dettagli del prodotto per inviare una richiesta all'amministratore per rendere il prodotto disponibile sul proprio marketplace privato. Le richieste software sono abilitate per impostazione predefinita e l'impostazione può essere modificata solo quando il marketplace privato è abilitato.

Quando il tuo marketplace privato è attivo, gli utenti finali possono acquistare solo i prodotti che hai approvato. Quando il tuo marketplace privato è disabilitato, conservi l'elenco dei prodotti. Tuttavia, la disabilitazione di un marketplace privato rimuove la restrizione per gli utenti dell'organizzazione. AWS Organizations Di conseguenza, possono abbonarsi a qualsiasi prodotto disponibile al pubblico.

Marketplace AWS

La creazione di un marketplace privato non interrompe l'esecuzione di Amazon Machine Images (AMI) attive su istanze Amazon Elastic Compute Cloud (Amazon EC2). Come best practice, assicurati che tutti i Marketplace AWS prodotti attualmente in uso nella tua organizzazione siano inclusi nel tuo marketplace privato. È inoltre consigliabile disporre di un piano per interrompere l'uso di prodotti non approvati prima di rendere attivo il marketplace privato. Dopo la pubblicazione del marketplace privato, tutti i nuovi abbonamenti o i rinnovi sono regolati dai prodotti approvati nel catalogo del marketplace privato.

Lavorare con prodotti privati

Alcuni prodotti non sono disponibili pubblicamente per la navigazione Marketplace AWS. Questi prodotti possono essere visualizzati solo quando ti viene offerta un'offerta privata dal venditore. L'offerta privata del venditore include un link al prodotto. Puoi aggiungere il prodotto al marketplace privato dal banner nella parte superiore della pagina.

Note

Se desideri abbonarti a un prodotto privato da un altro account della tua organizzazione, il venditore deve includere nell'offerta privata sia il tuo account Account AWS (per aggiungere il prodotto al marketplace privato) che quello dell'utente (per abbonarsi al prodotto).

Per rimuovere un prodotto privato dal tuo marketplace privato, devi [contattare l'Marketplace AWS Assistenza](#).

Gestione delle richieste degli utenti

Puoi consentire agli utenti di inviare richieste di prodotti da aggiungere al loro catalogo privato del marketplace con la funzione di richiesta software. Per farlo, accedi alla pagina dell'amministratore del tuo marketplace privato, seleziona Esperienze nel riquadro di navigazione a sinistra e scegli l'esperienza che desideri gestire. Dalla scheda Prodotti, scegli Richieste in sospeso. Da qui puoi esaminare le richieste fatte dagli utenti per l'aggiunta di prodotti al loro catalogo privato del marketplace.

Puoi aggiungere un numero qualsiasi di prodotti richiesti da questa pagina selezionando prima la casella di controllo accanto al nome di ciascun prodotto richiesto e quindi scegliendo **Aggiungi** a Private Marketplace. Allo stesso modo, puoi anche rifiutare una o più richieste selezionate scegliendo **Rifiuta**. Per visualizzare ulteriori informazioni su un prodotto (o sulla relativa richiesta software), scegli **Visualizza dettagli** nella colonna **Dettagli** relativa a quella richiesta.

Quando rifiuti una richiesta di prodotto, puoi aggiungere un motivo e impedire future richieste (blocco) per questo prodotto. Il blocco di un prodotto non ti impedirà di aggiungere il prodotto al tuo marketplace privato, ma impedirà agli utenti di richiederlo.

Archiviazione e riattivazione di un'esperienza di marketplace privata

Puoi rimuovere un'esperienza di marketplace privata archiviandola. Le esperienze archiviate non possono essere aggiornate o utilizzate per gestire gli account della tua organizzazione. Se hai dei segmenti di pubblico associati a un'esperienza archiviata, puoi associarli a un'esperienza diversa. Se decidi di utilizzare l'esperienza in un secondo momento, puoi sempre riattivarla. Gli amministratori degli account di gestione o gli amministratori delegati dispongono delle autorizzazioni per archiviare e riattivare le esperienze.

Note

Prima di archiviare un'esperienza, devi disabilitarla. Per informazioni sulla disabilitazione di un'esperienza, consulta [Configurazione](#) del marketplace privato.

Se attualmente sei un cliente di Private Marketplace e non disponi dell'AWS

Organizationsintegrazione per Private Marketplace, gli amministratori dell'account che ha creato l'esperienza dispongono delle autorizzazioni per archiviare e riattivare le esperienze.


Per archiviare una o più esperienze di marketplace private

1. Dalla pagina dell'amministratore di Private Marketplace, seleziona **Esperienze** nel riquadro di navigazione a sinistra.
2. Nella scheda **Esperienze attive**, seleziona una o più esperienze.
3. Scegli l'esperienza di archiviazione.

 Note

Se una o più esperienze hanno lo stato Live, devi portarle offline scegliendo Metti offline le esperienze.


4. Per verificare che desideri archiviare l'esperienza, digita **confirm** (tutto in minuscolo) nella casella di testo.
5. Scegliere Archive (Archivia).

 Note

Puoi anche archiviare un'esperienza selezionando l'esperienza, scegliendo Archivia esperienza in modalità Amministratore nella scheda Impostazioni e quindi scegliendo Salva.

Per riattivare una o più esperienze di marketplace private

1. Dalla pagina dell'amministratore di Private Marketplace, seleziona Esperienze nel riquadro di navigazione a sinistra.
2. Nella scheda Esperienze archiviate, seleziona una o più esperienze.
3. Scegli Riattiva.
4. Per verificare che desideri riattivare l'esperienza, digita **confirm** nella casella di testo.
5. Scegli Riattiva.

 Note

Puoi anche riattivare un'esperienza selezionando l'esperienza, scegliendo Riattiva esperienza in modalità Amministratore nella scheda Impostazioni e quindi scegliendo Salva.

Offerte private

La funzione di offerta privata del Marketplace AWS venditore ti consente di ricevere i prezzi dei prodotti e i termini dell'EULA da un venditore che non sono disponibili al pubblico. Negozi prezzi e condizioni con il venditore e il venditore crea un'offerta privata per l'AWSaccount da te indicato. Accetti l'offerta privata e inizi a ricevere il prezzo e le condizioni d'uso negoziati.

Ogni offerta privata prevede condizioni di prezzo e licenza specifiche per l'account dell'utente. Il venditore del prodotto ti offre un'offerta privata e l'offerta ha una data di scadenza prestabilita. Se non accetti l'offerta privata entro la data di scadenza, a seconda del tipo di prodotto a cui si riferisce l'offerta privata, verrai automaticamente trasferito all'offerta pubblica del prodotto o non sarai più abbonato al prodotto.

Se utilizzi la funzionalità di fatturazione consolidata in AWS Organizations, puoi accettare l'offerta privata dall'account di gestione dell'organizzazione o da un account membro. Se accetti dall'account di gestione, l'offerta privata può essere condivisa con tutti gli account dei membri dell'organizzazione. Gli account dei membri che erano precedentemente abbonati al prodotto devono inoltre accettare la nuova offerta privata per beneficiare dei prezzi. In alternativa, per i prodotti AMI e Container, puoi condividere la licenza dall'account di gestione agli account dei membri utilizzando AWS License Manager. Gli account dei membri che non erano precedentemente abbonati al prodotto devono accettare l'offerta privata per poter implementare il prodotto.

Per ulteriori informazioni sulla fatturazione consolidata, consulta [Consolidated Billing for Organizations nella AWS Billing Guida per l'utente](#). Di seguito sono riportati i punti chiave da ricordare quando inizi a utilizzare le tue offerte private.

- Marketplace AWS gli acquirenti possono accedere a servizi di finanziamento di terze parti per offerte private. Per ulteriori informazioni, vedi [Il finanziamento per i clienti è ora disponibile in Marketplace AWS](#).
- Non vi è alcuna differenza nel prodotto software acquistato utilizzando un'offerta privata. Il software acquistato tramite un'offerta privata si comporta come se lo acquistassi senza un'offerta privata.
- Gli abbonamenti ai prodotti acquistati con un'offerta privata vengono visualizzati come qualsiasi altro Marketplace AWS prodotto nella fattura mensile. Puoi utilizzare la fatturazione dettagliata per visualizzare l'utilizzo di ciascuno dei prodotti acquistati Marketplace AWS. Ciascuna delle tue offerte private ha una voce corrispondente a ciascun tipo di utilizzo.
- L'iscrizione a un'offerta privata non richiede il lancio di una nuova istanza del software. L'accettazione dell'offerta privata modifica il prezzo in modo che corrisponda al prezzo dell'offerta

privata. Se un prodotto offre il lancio con 1 clic, puoi implementare una nuova istanza del software. Se l'impostazione predefinita di un prodotto è il lancio con 1 clic, puoi accettare un'offerta privata senza avviare una nuova istanza. Per lanciarlo senza implementare una nuova istanza, scegli Avvio manuale nella pagina di evasione degli ordini. Puoi utilizzare la console Amazon Elastic Compute Cloud per distribuire istanze aggiuntive, proprio come faresti per altri prodotti.

Marketplace AWS

- Quando un venditore ti offre un'offerta privata, ricevi una conferma sull'account che il venditore ha incluso in un'offerta privata. Le offerte private sono collegate allo specifico account dell'acquirente del software indicato. Il venditore del software crea l'offerta privata per l'account specificato. Ogni offerta privata può essere effettuata su un massimo di 25 account.
- Quando accetti un'offerta privata, questa diventa un accordo (noto anche come contratto o abbonamento) tra te e il venditore.
- I venditori possono offrirti di aggiornare o rinnovare l'acquisto di un contratto SaaS o di un contratto SaaS con prodotto di consumo. [Ad esempio, un venditore può creare una nuova offerta privata per concedere nuovi diritti, offrire sconti sui prezzi, modificare i piani di pagamento o modificare il contratto di licenza con l'utente finale \(EULA\) per utilizzare condizioni di licenza standardizzate.](#)

Questi rinnovi o upgrade sono modifiche all'offerta privata originale che hai accettato e utilizzi la stessa procedura per accettarli. Se accetti la nuova offerta privata di aggiornamento o rinnovo, i nuovi termini del contratto entrano in vigore immediatamente, senza alcuna interruzione del servizio software. Eventuali termini precedenti o pagamenti programmati rimanenti vengono annullati e sostituiti dai termini del nuovo contratto.

- Puoi controllare tutti gli abbonamenti software annuali nella Marketplace AWS sezione Il tuo software. Se un abbonamento annuale viene acquistato da un account utilizzando AWS Organizations la fatturazione consolidata, viene condiviso tra l'intera famiglia di account collegati. Se l'account di acquisto non ha istanze in esecuzione, l'abbonamento annuale viene conteggiato nell'utilizzo in un altro account collegato che esegue quel software. Per ulteriori informazioni sugli abbonamenti annuali, consulta [the section called "Elenchi AMI"](#)
- Quando un'offerta privata scade, non puoi sottoscriverla. Tuttavia, puoi contattare il venditore. Chiedi al venditore di modificare la data di scadenza dell'offerta corrente con una data futura o di creare una nuova offerta privata per te.

Tipi di prodotto idonei per le offerte private

Puoi ricevere offerte private per i seguenti tipi di prodotto.

Tipo di offerta	Descrizione
Prodotti di dati	Per ulteriori informazioni, consulta Accettazione di un'offerta privata nella Guida per l'utente di AWS Data Exchange.
Contratto SaaS	<p>Con un contratto Software as a Service (SaaS), puoi impegnarti a pagare in anticipo per l'utilizzo o previsto di un prodotto SaaS o negoziare un piano di pagamento flessibile con il venditore . La durata del contratto è di un mese, un anno, due anni o tre anni, oppure seleziona una durata personalizzata in mesi, fino a 60 mesi. Se ti impegni a effettuare un pagamento anticipato, ti verrà addebitato in anticipo l'utilizzo o del software del prodotto.</p> <p>Se il venditore offre un piano di pagamento flessibile, ti verranno fatturati in base alle date del piano di pagamento in base agli importi indicati nell'offerta privata.</p> <p>Il venditore può inoltre includere pay-as-you-go prezzi concordati per un utilizzo superiore a quello previsto dal contratto.</p>
Abbonamento SaaS	Con un abbonamento SaaS, l'utente accetta un prezzo per l'utilizzo di un prodotto. Il venditore monitora e segnala l'utilizzo da Marketplace AWS parte tua e ti viene fatturato il costo di ciò che utilizzi.
AMI ogni ora	Con Amazon Machine Image (AMI) hourly, puoi negoziare una tariffa oraria per l'utilizzo di un'AMI, arrotondata all'ora più vicina.
AMI ogni ora con annuale	Con AMI hourly with annual, puoi negoziare i prezzi orari e a lungo termine per tipo di

Tipo di offerta	Descrizione
	<p>istanza. I prezzi a lungo termine si riferiscono alla durata dell'offerta privata, che può variare da 1 giorno a 3 anni. Se il venditore crea un'offerta privata senza un programma di pagamento flessibile, puoi eseguire istanze Amazon EC2 al prezzo orario determinato nell'offerta privata e, facoltativamente, acquistare e impegni anticipati per la durata del contratto al prezzo a lungo termine stabilito nell'offerta privata. Se il venditore crea un'offerta privata con un piano di pagamento flessibile, ti verranno fatturate le date del piano di pagamento per gli importi indicati nell'offerta privata indipendentemente dall'utilizzo. In questo tipo di offerta privata, il venditore può includere una serie di istanze Amazon EC2 per tipo di istanza che puoi eseguire senza che ti venga addebitato il prezzo orario. Qualsiasi utilizzo superiore a quanto incluso viene quindi addebitato al prezzo orario stabilito nell'offerta privata.</p>

Tipo di offerta	Descrizione
Contratto AMI	Con i contratti AMI, si negozia il prezzo del contratto e la durata del contratto, che può essere compresa tra 1 e 60 mesi. Se il venditore crea un'offerta privata senza un programma di pagamento flessibile, al momento dell'accettazione, puoi configurare il contratto in base al prezzo e alle opzioni stabilite nell'offerta privata. Se il venditore crea un'offerta privata con un piano di pagamento flessibile, le date del piano di pagamento ti verranno fatturate in base agli importi indicati nell'offerta privata. In questo tipo di offerta privata, il venditore configura il contratto nell'offerta privata e non può essere configurato al momento dell'accettazione.
Prodotti in contenitore	Con i prodotti container, puoi negoziare i prezzi orari o annuali per i prodotti container che utilizzi, per pod, task o unità personalizzata, in base al prodotto che stai acquistando. Le offerte private dei prodotti container corrispondono alle offerte private dei prodotti AMI.
Prodotti per l'apprendimento automatico	Le offerte private possono consistere in un contratto con una tariffa anticipata fissa per un determinato numero di giorni. Alla fine del contratto, tutte le istanze che continuano a funzionare vengono fatturate alla tariffa oraria stabilita dal venditore nell'offerta privata.
Servizi professionali	Tutte le offerte di servizi professionali sono offerte private. È necessario collaborare con l'acquirente per creare l'offerta privata. Per ulteriori informazioni, consulta Prodotti per servizi professionali .

Prepararsi ad accettare un'offerta privata

Quando si negozia una tipica offerta privata, si paga l'intero importo dell'offerta al momento dell'accettazione, a meno che non si utilizzi un finanziamento da parte di terzi. Con il finanziamento tramite terzi, il finanziatore paga il contratto per vostro conto e vi fattura in base al piano di pagamento concordato. Prima di accettare un'offerta privata, verificate la struttura di fatturazione della vostra azienda, il metodo di pagamento per la AWS fatturazione e le impostazioni fiscali.

Verifica delle tue preferenze AWS Billing and Cost Management

Billing and Cost Management è il servizio che utilizzi per pagare AWS la bolletta, monitorare l'utilizzo e pianificare i costi. Puoi utilizzare la funzionalità di fatturazione consolidata AWS Organizations per consolidare fatturazione e pagamento per più account o più account Amazon Internet Services Pvt. Ltd (AISPL). Ogni organizzazione AWS Organizations dispone di un account di gestione che paga gli addebiti di tutti gli account dei membri. L'account di gestione è denominato account di pagamento e l'account membro è denominato account collegato. Prima di negoziare un'offerta privata, verificate in che modo la vostra azienda paga la AWS bolletta e su quale AWS conto viene presentata l'offerta privata.

Verifica del metodo di pagamento

Prima di accettare un'offerta privata, verifica che il tuo metodo di pagamento supporti il pagamento dell'intero costo dell'offerta privata. Per verificare il metodo di pagamento, apri la console Billing and Cost Management [all'indirizzo](https://console.aws.amazon.com/billing/) <https://console.aws.amazon.com/billing/>.

Verifica delle impostazioni fiscali

Se la tua azienda ha i requisiti per l'esenzione fiscale, verifica le impostazioni fiscali. Per visualizzare o modificare le impostazioni fiscali, accedi a AWS Management Console e, nelle impostazioni del tuo account, visualizza le impostazioni fiscali. Per ulteriori informazioni sulla registrazione fiscale, consulta [Come posso aggiungere o aggiornare il mio codice fiscale o l'indirizzo legale aziendale per il mio account AWS?](#) .

Visualizzazione e sottoscrizione di un'offerta privata

Puoi visualizzare un'offerta privata in uno dei seguenti modi:

Argomenti

- [Visualizzazione e sottoscrizione a un'offerta privata da un elenco di offerte private](#)
- [Visualizzazione e sottoscrizione di un'offerta privata tramite un link fornito dal venditore](#)
- [Visualizzazione e sottoscrizione di un'offerta privata dalla pagina del prodotto](#)

Visualizzazione e sottoscrizione a un'offerta privata da un elenco di offerte private

Per visualizzare e sottoscrivere un'offerta privata da un elenco di offerte private esteso al tuo Account AWS

1. Accedi alla console [Marketplace AWS](#).
2. Vai alla [pagina delle offerte private](#).
3. Dalla pagina Offerte private, nella scheda Offerte disponibili, seleziona l'ID dell'offerta per l'offerta che ti interessa.
4. Visualizza e sottoscrivi l'offerta privata.

Visualizzazione e sottoscrizione di un'offerta privata tramite un link fornito dal venditore

Per visualizzare e sottoscrivere un'offerta privata tramite un link che ti è stato inviato dal venditore

1. Accedi alla console [Marketplace AWS](#).
2. Segui il link inviato dal venditore per accedere direttamente all'offerta privata.

Note

Se segui questo link prima di accedere all'account corretto, verrà visualizzato un errore Pagina non trovata (404).

Per ulteriori informazioni, consulta [Quando faccio clic sull'ID dell'offerta per visualizzare l'offerta privata, ricevo l'errore Page not found \(404\)](#).

3. Visualizza e sottoscrivi l'offerta privata.

Visualizzazione e sottoscrizione di un'offerta privata dalla pagina del prodotto

Per visualizzare e sottoscrivere un'offerta privata dalla pagina del prodotto

1. Accedi alla console [Marketplace AWS](#).
2. Vai alla pagina del prodotto corrispondente.
3. Visualizza il banner nella parte superiore della pagina che mostra l'offerta privata, l'ID dell'offerta e la scadenza dell'offerta.

Note

Le offerte private con data futura sono elencate come rinnovi anticipati. Per ulteriori informazioni, consulta [the section called "Lavorare con accordi con date future"](#).

4. Seleziona l'ID dell'offerta.
5. Visualizza e sottoscrivi l'offerta privata.

Note

Se hai più di un'offerta privata per quel prodotto, ogni offerta viene visualizzata sotto Nome dell'offerta. Se hai un contratto in corso per quel prodotto, accanto all'offerta viene visualizzata un'icona In uso.

Risoluzione dei problemi relativi alle offerte private

Se riscontri problemi relativi al codice di stato HTTP 404 (Not Found) o difficoltà simili quando lavori con le offerte private inMarketplace AWS, consulta gli argomenti di questa sezione.

Problemi

- [Quando faccio clic sull'ID dell'offerta per visualizzare l'offerta privata, ricevo l'errore Page not found \(404\)](#)
- [Nessuno di questi suggerimenti funziona](#)

Quando faccio clic sull'ID dell'offerta per visualizzare l'offerta privata, ricevo l'errore Page not found (404)

- Verifica di aver effettuato l'accesso nel modo corretto Account AWS. Il venditore estende le offerte private a Account AWS ID specifici.
- Verifica se l'offerta esiste nella sezione [Offerte private](#) della Marketplace AWS console. Se non trovi l'offerta nella sezione Offerte private, è possibile che il venditore abbia esteso l'offerta a un Account AWS ID diverso. Rivolgiti al venditore per confermare l'Account AWSID a cui è stata estesa l'offerta.
- Verifica che l'offerta privata non sia scaduta visualizzando la scheda Offerte accettate e scadute in [Offerte private](#) nella Marketplace AWS console. Se l'offerta è scaduta, contatta il venditore per modificare la data di scadenza dell'offerta o estendere una nuova offerta al tuo account.
- Verifica che l'ID dell'account sia inserito nell'elenco consentito per visualizzare l'offerta privata. Alcuni ISV utilizzano offerte limitate. Chiedi all'ISV se ha inserito il tuo account nella lista consentita per visualizzare il prodotto. L'elenco consentito è necessario per le offerte limitate di prodotti AMI. Se lavori in un'AWSorganizzazione e il venditore estende l'offerta all'account di gestione, gli account collegati devono essere inseriti nella lista consentita per iscriversi. In caso contrario, gli account collegati dell'acquirente che non sono nella lista consentita riceveranno l'errore Pagina non trovata (404) quando tenteranno di visualizzare l'offerta.
- Rivolgiti al tuo AWS amministratore per confermare di disporre delle autorizzazioni `aws-marketplace:ViewSubscriptions` IAM se devi visualizzare l'offerta. Per ulteriori informazioni sulla Marketplace AWS sicurezza, consulta [Sicurezza attiva Marketplace AWS](#).
- Verifica se stai utilizzando un marketplace privato.
 - Assicurati che il prodotto sia nell'elenco dei prodotti consentiti del tuo marketplace privato (se applicabile), in modo da poterlo acquistare. Se non sei sicuro, contatta l'amministratore di sistema per verificare.

Nessuno di questi suggerimenti funziona

Se nessuno dei suggerimenti precedenti ha risolto l'errore 404 (Not Found) del codice di stato HTTP, prova le seguenti azioni nel tuo browser:

- Svuota la cache.
- Eliminare i cookie.
- Esci, quindi accedi nuovamente.

- Usa una modalità di navigazione in incognito o privata.
- Prova un altro browser. Non è consigliabile utilizzare Internet Explorer.

Se hai completato tutti i suggerimenti per la risoluzione dei problemi e continui a ricevere l'errore Pagina non trovata, invia un messaggio e-mail a <mpcustdesk@amazon.com> per ricevere assistenza.

Pagina delle offerte private in Marketplace AWS

Nella Marketplace AWS pagina delle offerte private sono elencate tutte le offerte private che sono state estese Account AWS ai tuoi prodotti sia privati che pubblici. Tutte le offerte a tua disposizione vengono visualizzate per ogni prodotto. Puoi accettare un'offerta per ogni prodotto.

Comprendere la pagina delle offerte private

Puoi visualizzare la pagina delle offerte private accedendo alla Marketplace AWS console e accedendo alla sezione Offerte private. Le offerte private estese a te Account AWS sono elencate nella sezione Offerte private e includono l'ID dell'offerta, il prodotto, il venditore registrato (ISV o partner di canale), l'editore, gli accordi attivi (se applicabili) e la data di scadenza dell'offerta. Puoi selezionare l'ID dell'offerta per l'offerta di interesse per visualizzare i dettagli dell'offerta e sottoscrivere un'offerta privata.

La pagina delle offerte private include le seguenti informazioni:

- La scheda Offerte disponibili elenca le offerte private estese al tuo account che puoi accettare. Il link ID dell'offerta in questa scheda è lo stesso link che il venditore potrebbe averti fornito per accedere ai dettagli dell'offerta privata.
- La scheda Offerte accettate e scadute elenca le offerte che hai accettato e che hanno portato alla creazione di un accordo. Elenca anche le offerte che hanno raggiunto la data di scadenza dell'offerta stabilita dal venditore. Questa scheda può essere utile per recuperare l'ID dell'offerta e il numero del contratto precedenti (se disponibili) al momento del rinnovo con un venditore. Se l'offerta ha portato a un accordo e l'accordo è attivo, puoi scegliere il contratto per visualizzare la pagina dei dettagli dell'abbonamento.

Note

Le offerte private con data futura sono elencate come Rinnovi anticipati. Per ulteriori informazioni, consulta [the section called “Lavorare con accordi con date future”](#).

Per ulteriori informazioni sulla modifica, l'aggiornamento o il rinnovo di un'offerta privata, consulta [Modifica o annullamento dell'iscrizione a un'offerta privata](#)

Autorizzazioni necessarie per visualizzare la pagina delle offerte private

Per visualizzare la pagina delle offerte private nella Marketplace AWS console, devi disporre delle seguenti autorizzazioni:

- Se utilizzi politiche AWS gestite: `AWSMarketplaceRead-onlyAWSMarketplaceManageSubscriptions`, o `AWSMarketplaceFullAccess`
- Se non utilizzi policy AWS gestite: IAM action `aws-marketplace:ListPrivateListings` e `aws-marketplace:ViewSubscriptions`

Se non riesci a visualizzare la pagina delle offerte private, contatta il tuo amministratore per configurare le autorizzazioni AWS Identity and Access Management (IAM) corrette. Per ulteriori informazioni sulle autorizzazioni IAM necessarie per Marketplace AWS, consulta [AWSpolitiche gestite per Marketplace AWS gli acquirenti](#)

Abbonamento a un'offerta privata SaaS

Per un'offerta privata di software as a service (SaaS), le opzioni di configurazione disponibili dipendono dal contratto che potresti negoziare con il venditore.

Come illustrato nel diagramma seguente, la pagina dell'offerta privata include le seguenti sezioni:

- Nome dell'offerta: questo è il nome che il venditore ha dato alla tua offerta privata al momento della creazione.
- Informazioni di fatturazione consolidate: questa notifica viene visualizzata se utilizzi la fatturazione consolidata con il tuo Account AWS
- Specifiche e durata del contratto: questo riquadro mostra la durata dell'offerta e le dimensioni che definiscono l'offerta. Le dimensioni descrivono come viene misurato l'utilizzo e per quanto tempo

rimane in vigore il prezzo negoziato: ad esempio, 5 GB/giorno per 12 mesi o 0,01 USD per utente all'ora. Se l'offerta privata è un contratto, paghi per un importo di utilizzo concordato per tutta la durata del contratto. Se l'offerta privata è un abbonamento, paghi per l'utilizzo misurato alla tariffa concordata.

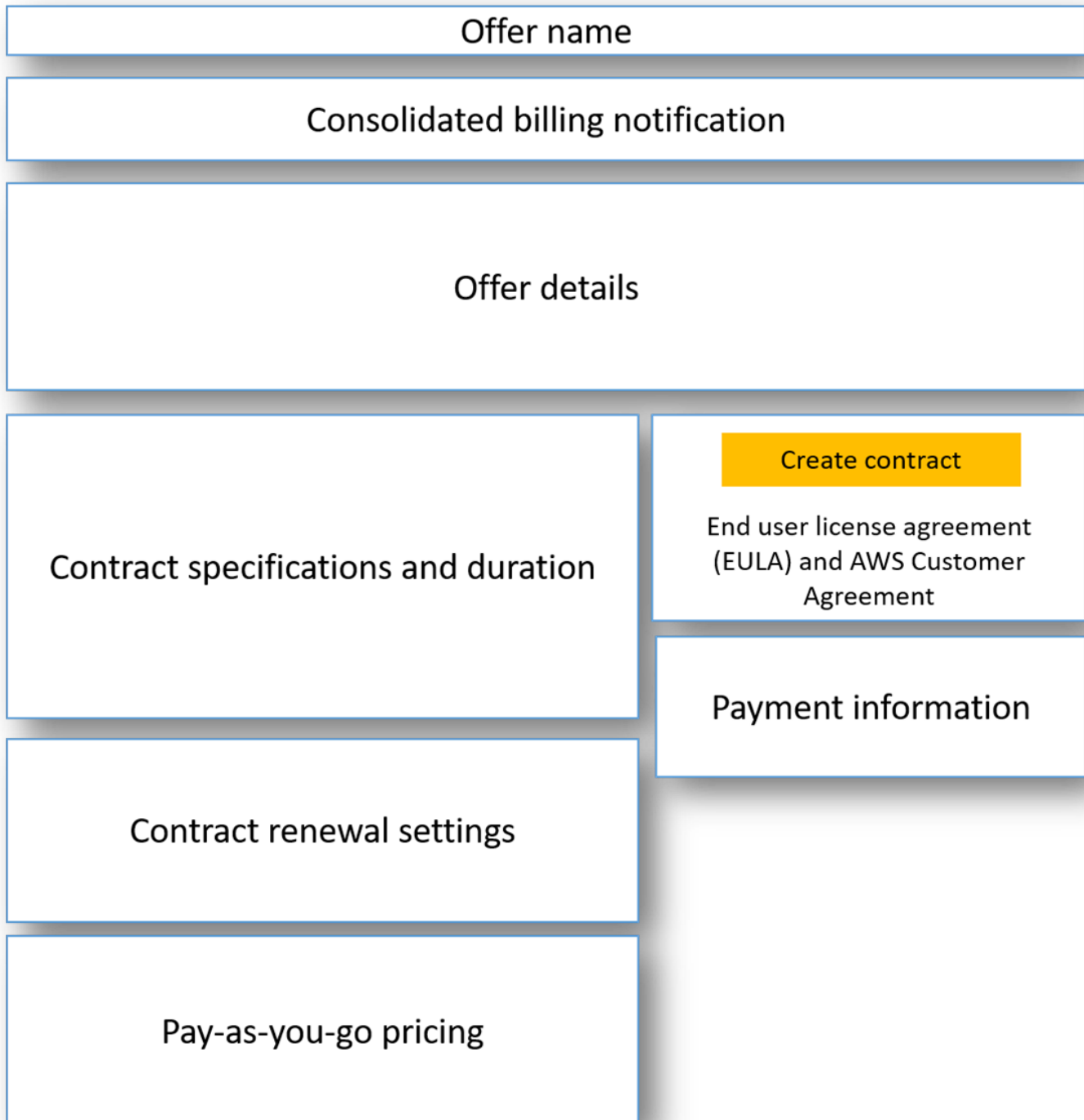
Note

Le offerte private con data futura sono elencate come Rinnovi anticipati. Per ulteriori informazioni, consulta [the section called “Lavorare con accordi con date future”](#).

- Impostazioni per il rinnovo del contratto: non puoi impostare il rinnovo automatico delle offerte private. Per le offerte private sui prodotti SaaS, questo riquadro indica sempre che non è previsto alcun rinnovo per questa offerta.
- ay-as-you-go Prezzi P: se negoziate prezzi per l'utilizzo del prodotto oltre a quelli definiti nella vostra offerta privata, le specifiche relative ai costi di utilizzo aggiuntivi vengono visualizzate qui. Ad esempio, se hai sottoscritto un contratto SaaS per l'archiviazione di dati di 5 GB/giorno per 12 mesi e utilizzi 10 GB/giorno, i primi 5 GB rientrano nel contratto. I 5 GB aggiuntivi al giorno vengono addebitati al prezzo. pay-as-you-go Con gli abbonamenti SaaS, hai una tariffa concordata per l'utilizzo che utilizzi durante la durata del contratto.
- Contratto di licenza con l'utente finale (EULA) e pulsante per la creazione del contratto: qui puoi visualizzare il contratto di licenza che il venditore ha caricato per questa offerta privata. Qui puoi anche accettare il contratto dopo aver visualizzato tutte le specifiche dell'offerta privata e essere pronto a stipulare il contratto.
- Informazioni sul pagamento: questo riquadro descrive quando il pagamento è dovuto e, se è stato negoziato un piano di pagamento, la data e gli orari in cui il pagamento è dovuto.

Important

Se una sezione non viene visualizzata nella pagina dell'offerta privata, non è una parte negoziata dell'offerta privata.



Per sottoscrivere un'offerta privata SaaS

1. Segui i passaggi per [Visualizzazione e sottoscrizione di un'offerta privata](#).

2. Nel riquadro dei dettagli dell'offerta, verifica di aver scelto l'offerta privata corretta. Potresti avere più offerte per il prodotto.
3. Nel riquadro Specifiche e durata del contratto, verifica che la durata del contratto e i dettagli del contratto corrispondano a quelli negoziati. In caso contrario, verifica di aver selezionato l'offerta privata corretta o contatta il venditore che ha creato l'offerta.

Note

Le offerte private con data futura sono elencate come Rinnovi anticipati. Per ulteriori informazioni, consulta [the section called "Lavorare con accordi con date future"](#).

4. Se hai negoziato pay-as-you-go i prezzi, dovrebbe esserci un riquadro con informazioni che descrivano i termini negoziati. Verifica le informazioni o, se mancano (e te le aspetti), contatta il venditore.
5. Nel riquadro delle informazioni di pagamento, verifica le informazioni di pagamento. Se hai negoziato un piano di pagamento flessibile, vengono elencate le date e gli importi dei pagamenti. In caso contrario, l'importo totale del contratto viene fatturato al momento dell'accettazione dell'offerta.
6. Nel riquadro EULA e creazione del contratto, verifica che l'EULA sia quello negoziato con il venditore. Dopo aver esaminato tutti i termini e le condizioni del contratto, scegli Crea contratto per accettare l'offerta.

Dopo aver accettato l'offerta, si apre una pagina di conferma che indica che l'iscrizione al prodotto è avvenuta con successo. Scegli Configura il tuo account per essere reindirizzato alla pagina del venditore e completa la configurazione del tuo account sul sito web del venditore.

Iscrizione a un'offerta privata AMI

Le sezioni e le opzioni di configurazione disponibili per la tua offerta privata Amazon Machine Image (AMI) dipendono dal contratto negoziato con il fornitore del prodotto. L'immagine seguente mostra il layout di una pagina di offerta privata AMI sul Marketplace AWS sito web.

Come mostrato nel grafico seguente, la regione. L'offerta privata include le seguenti sezioni:

- Nome e prodotto del fornitore: si tratta del nome del fornitore e del prodotto a cui è destinata l'offerta privata. Sulla destra c'è il pulsante di configurazione del prodotto.

- Guida alla pagina: quest'area contiene indicazioni per completare le attività sulla pagina e accettare l'offerta privata.
- Termini e condizioni: questa sezione include le seguenti informazioni:
 - In alto a sinistra c'è il nome dell'offerta privata e un'etichetta che indica che si tratta di un'offerta privata.
 - Sotto la sezione relativa al nome dell'offerta privata c'è una notifica di accettazione del contratto. Puoi utilizzare il pulsante Accetta contratto per accettare l'offerta privata.
 - Sotto la sezione relativa alle notifiche sono disponibili le sezioni relative alla durata del contratto, ai componenti inclusi nel contratto e al prezzo delle istanze negoziato, oltre a un'altra opportunità per visualizzare o scaricare l'EULA.
- Durata dei termini: questa sezione mostra il numero di giorni del contratto e la data di fine del contratto.
- Informazioni aggiuntive sull'offerta: sulla destra ci sono immagini in miniatura del prezzo totale del contratto, del prossimo pagamento programmato, dei termini attuali e di altre offerte pubbliche e private disponibili.

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


Abbonamento a un'offerta privata AMI annuale con un programma di pagamento flessibile

Per abbonarsi a un'offerta privata AMI, è necessario accettare l'offerta privata sul Marketplace AWS sito web. Non possibile accettare l'offerta privata sulla Marketplace AWS console Elastic Compute Cloud (Amazon EC2). Se il venditore crea un'offerta privata con un piano di pagamento flessibile, ti verranno fatturati in base alle date del piano di pagamento gli importi indicati nell'offerta privata. Per accettare un'offerta privata AMI con un programma di pagamento flessibile, utilizza la seguente procedura.

Accettare un'offerta privata AMI con un programma di pagamento flessibile

1. Segui i passaggi per [Visualizzazione e sottoscrizione di un'offerta privata](#).

2. Verifica di aver visualizzato l'offerta privata corretta. Il fornitore può creare per te più offerte private per il suo prodotto. Eventuali offerte private aggiuntive vengono visualizzate nella sezione Altre offerte disponibili.
3. Verifica che la data di scadenza dell'offerta e le informazioni sui prezzi siano quelle negoziate per l'offerta privata. In caso contrario, verificare di aver visualizzato l'offerta privata corretta.
4. Scarica l'EULA e verifica che sia quello che hai negoziato per l'offerta privata.
5. Nella sezione Durata dei termini, verifica che i termini dell'offerta privata siano quelli che hai negoziato.
6. Dopo aver verificato i dettagli dell'offerta privata, nella sezione Termini e condizioni, scegli Accetta contratto.
7. Rivedi i termini e scegli Conferma se accetti.

 Important

Non aggiorni il browser mentre il sistema elabora la richiesta del contratto.

Quando vuoi configurare l'AMI, scegli Continue to Configurare (Continua con la configurazione). È necessario completare la procedura di abbonamento per ogni utilizzo del prodotto.

Abbonamento a un'offerta privata AMI annuale senza un programma di pagamento flessibile

Per abbonarsi a un'offerta privata AMI, è necessario accettare l'offerta privata sul Marketplace AWS sito web. Non puoi accettarlo dalla Marketplace AWS console Amazon EC2. Se il venditore crea un'offerta privata senza un piano di pagamento flessibile, al momento dell'accettazione, puoi configurare il contratto in base al prezzo e alle opzioni impostati nell'offerta privata. Per accettare un'offerta privata AMI senza un programma di pagamento flessibile, utilizza la seguente procedura.

Accettare un'offerta privata AMI senza un programma di pagamento flessibile

1. Verifica di aver visualizzato l'offerta privata corretta. Il fornitore può creare per te più offerte private per il suo prodotto. Eventuali offerte private aggiuntive vengono visualizzate nel riquadro delle offerte private aggiuntive. Verifica che l'offerta che desideri accettare sia visualizzata come Visualizzazione dell'offerta.

Note

In molti casi, l'account del pagatore non è l'account che utilizza il prodotto. Ti consigliamo di avviare il prodotto manualmente anziché selezionare l'opzione con un clic se accetti l'offerta utilizzando l'account del pagatore.

2. Verifica che la data di scadenza dell'offerta e le informazioni sui prezzi siano quelle negoziate per l'offerta privata. In caso contrario, verificare di aver visualizzato l'offerta privata corretta.
3. Scarica l'EULA e verifica che sia quello che hai negoziato per l'offerta privata.
4. Nel riquadro delle condizioni del contratto, verifica che i termini dell'offerta privata siano quelli che hai negoziato.
5. Verifica che i dettagli dell'offerta corrispondano a quelli che hai negoziato per l'offerta privata, quindi scegli Accetta i termini. In caso contrario, verificare di aver visualizzato l'offerta privata corretta.
6. Per Iscriviti a questo software, per Tipo di istanza, scegli dall'elenco dei tipi di istanza disponibili. In Quantità, scegli il numero di licenze.
7. Controlla dei gruppi. Quando sei soddisfatto, scegli Crea contratto, quindi scegli Conferma.

Quando vuoi configurare l'AMI, scegli Continue to Configurare (Continua con la configurazione). È necessario completare la procedura di abbonamento per ogni utilizzo del prodotto.

Modifica o annullamento dell'iscrizione a un'offerta privata

Puoi passare dagli abbonamenti standard alle offerte private e puoi anche modificare alcune offerte private esistenti in Marketplace AWS. Il processo varia in base all'accordo in vigore.

Per molti abbonamenti, quando si passa da un'offerta pubblica a un'offerta privata, si negozia l'offerta con l'ISV o il partner di canale. Dopo aver accettato l'offerta privata, il relativo abbonamento o gli abbonamenti esistenti passano automaticamente al modello di prezzo dell'offerta privata. Ciò non richiede ulteriori azioni da parte tua. Utilizza le seguenti indicazioni per identificare il tuo scenario e i passaggi per iniziare a ricevere i prezzi della tua offerta privata.

Passaggio dai prezzi delle offerte pubbliche a quelli privati

Dopo aver accettato l'offerta privata, non sono necessarie ulteriori azioni per l'utente che ha accettato l'offerta. Vengono passati ai prezzi, ai termini e alle condizioni definiti nell'offerta privata. Per passare

ai prezzi, ai termini e alle condizioni dell'offerta privata, ogni utente collegato che utilizza il prodotto deve accettare l'offerta privata. Qualsiasi utente che inizi a utilizzare il prodotto deve inoltre accettare l'offerta privata per ottenere i prezzi, i termini e le condizioni definiti nell'offerta privata.

Modifica di un contratto SaaS: aggiornamenti e rinnovi

Questa sezione si applica al contratto Software as a Service (SaaS) e al contratto SaaS con prodotti di consumo. Se hai stipulato un contratto attivo in base a una precedente offerta privata e desideri accettare una nuova offerta privata per lo stesso prodotto, il venditore può aggiornare o rinnovare il contratto esistente per modificare i termini, i prezzi o la durata o rinnovare il contratto esistente prima della scadenza. Ciò comporterà una nuova offerta privata da accettare, senza dover prima annullare il contratto esistente.

Note

Le offerte private con data futura sono elencate come Rinnovi anticipati. Per ulteriori informazioni, consulta [the section called “Lavorare con accordi con date future”](#).

Per accettare un upgrade o un rinnovo, devi rispettare le condizioni di fatturazione. Se al momento non rispetti i termini di fatturazione, invia una richiesta al [Servizio AWS Clienti](#) per modificare il metodo di pagamento in fatturazione.

Se non desideri passare alla fatturazione, puoi intraprendere una delle seguenti azioni:

- Collabora con il fornitore del prodotto e il team di assistenza Marketplace AWS clienti per annullare il contratto in corso prima di accettare una nuova offerta privata per quel prodotto
- Accetta l'offerta su un altro Account AWS.

Passaggio da un abbonamento SaaS a un contratto SaaS

Per passare da un abbonamento SaaS a un contratto SaaS, devi prima annullare l'iscrizione all'abbonamento SaaS. Quindi accetti l'offerta privata per il contratto SaaS. Per visualizzare gli abbonamenti SaaS esistenti, scegli Your Marketplace Software nell'angolo in alto a destra della console. Marketplace AWS

Passaggio da un contratto AMI a un nuovo contratto

Se disponi di un contratto Amazon Machine Image (AMI) in base a una precedente offerta privata e desideri accettare una nuova offerta privata per lo stesso prodotto, devi effettuare una delle seguenti operazioni:

- Attendi la scadenza del contratto AMI corrente prima di accettare il nuovo contratto AMI.
- Collabora con il fornitore del prodotto e il team di Marketplace AWS assistenza clienti per recedere dal contratto in corso.
- Accetta l'offerta privata utilizzando un'offerta diversa Account AWS da quella contrattuale

Passaggio da AMI a cadenza oraria a AMI annuale

Quando si passa da un abbonamento orario AMI a un abbonamento annuale AMI, l'abbonamento funziona in modo simile a un sistema di voucher. Ogni ora di utilizzo dell'AMI è compensata da un'unità nell'abbonamento annuale AMI. Quando si acquista l'abbonamento annuale tramite un'offerta privata, tutti gli account associati abbonati al prodotto passano automaticamente al prezzo negoziato nell'offerta privata. Gli account collegati che iniziano un abbonamento dopo l'entrata in vigore dell'offerta privata devono sottoscrivere l'offerta privata al momento dell'iscrizione.

Note

Le licenze annuali della vecchia offerta vengono disattivate immediatamente dopo l'accettazione dei termini della nuova offerta. Collaborate con l'ISV per discutere della compensazione per le vecchie licenze e di come procedere con la nuova offerta.

Passaggio dall'AMI annuale all'AMI ogni ora

Alla scadenza dell'abbonamento annuale, tutti gli account collegati abbonati al prodotto vengono automaticamente passati alla tariffa oraria AMI. Se è in vigore un abbonamento annuale, l'account collegato non può passare a un abbonamento orario per quel prodotto senza annullare l'abbonamento.

Lavorare con accordi e offerte private con date future

Con gli accordi con data futura (FDA) Marketplace AWS, puoi abbonarti a prodotti il cui utilizzo del prodotto inizia in una data futura. Puoi gestire quando acquisti un prodotto indipendentemente da quando paghi e quando utilizzi il prodotto.

La FDA aiuta gli acquirenti a eseguire le seguenti azioni in modo indipendente per le transazioni su Marketplace AWS:

- Acquista il prodotto/prenota l'offerta accettando l'offerta.
- Inizia a utilizzare il prodotto (attivazione della licenza/autorizzazione).
- Paga un acquisto (generazione della fattura).

La FDA è supportata nelle offerte private, nella creazione di prodotti SaaS (Software as a Service), nei contratti e nei contratti con prezzi al consumo (CCP) e con o senza pagamenti flessibili.

Quando utilizzi accordi con date future, tieni presente le seguenti date:

Data di firma dell'accordo

La data in cui hai accettato l'offerta e in cui è stato creato l'accordo. Questa data indica la data di creazione dell'ID dell'accordo.

Data di inizio dell'accordo

La data di inizio dell'utilizzo del prodotto. Questa è la data futura o la data di inizio futura. Questa è la data di attivazione della licenza/autorizzazione.

Data di fine del contratto

Data di scadenza del contratto. Il contratto e la licenza/diritto scadono in questa data.

Per ulteriori informazioni sull'utilizzo degli FDA, consulta i seguenti argomenti:

Argomenti

- [Creazione di accordi con data futura](#)
- [Utilizzo di uno strumento di pianificazione dei pagamenti flessibile con accordi con date future](#)
- [Modifica dei contratti con data futura](#)
- [Ricezione di notifiche per accordi con date future](#)

Creazione di accordi con data futura

Per i contratti SaaS e i contratti con prezzi al consumo, con e senza un programma di pagamento flessibile, il venditore stabilisce la data di inizio del contratto come parte della generazione di un'offerta privata. In qualità di acquirente, devi collaborare con i venditori per assicurarti che la data di inizio soddisfi i tuoi requisiti.

Per creare un accordo con date future, utilizzare la procedura seguente. Puoi visualizzare gli accordi con data futura nella Marketplace AWS console nella pagina Gestisci abbonamenti.

Per creare un accordo con data futura

1. Segui i passaggi per [Visualizzazione e sottoscrizione di un'offerta privata](#).
2. Nel riquadro dei dettagli dell'offerta, verifica di aver scelto l'offerta privata corretta e che la data di inizio del contratto sia corretta. Le offerte con data futura sono contrassegnate come Rinnovi anticipati nel menu a discesa Offerta.

Note

Per i prodotti SaaS, alla data di inizio del contratto, devi assicurarti di completare la configurazione del tuo account presso l'ISV. Non puoi completare questo passaggio prima della data di inizio del contratto. Per ulteriori informazioni, consultare [the section called "Abbonamento a un'offerta privata SaaS"](#)

Utilizzo di uno strumento di pianificazione dei pagamenti flessibile con accordi con date future

Puoi utilizzare lo strumento di pianificazione dei pagamenti flessibile con accordi con date future. Puoi impostare i pagamenti per gli acquisti in un momento a tua scelta tra la data di firma del contratto e la data di fine del contratto. Questo approccio include i pagamenti prima e dopo la data di inizio del contratto.

Il venditore registrato che crea l'offerta privata sceglie le date e gli importi di pagamento. Per maggiori dettagli, consulta [Flexible Payment Scheduler](#).

Modifica dei contratti con data futura

È possibile aumentare le unità acquistate di una determinata dimensione presso la FDA prima e dopo la data di inizio del contratto. Questa opzione è possibile quando il contratto non prevede un calendario di pagamento flessibile. Per maggiori dettagli, consulta [Flexible Payment Scheduler](#).

L'importo proporzionale ti verrà addebitato alla data di inizio del contratto, una volta completata la modifica. Se la tua data di inizio è passata, ti verrà addebitato immediatamente.

Ricezione di notifiche per accordi con date future

Riceverai notifiche e-mail inviate all'account root designato per le seguenti azioni intraprese sui contratti con data futura:

- Accettazione dell'offerta/creazione del contratto (data di firma del contratto)
- Al momento dell'attivazione della licenza o del diritto (data di inizio del contratto)
- Promemoria per contratti in scadenza con 30, 60 o 90 giorni di anticipo
- Scadenza del contratto (data di fine del contratto)
- In caso di modifica o sostituzione del contratto

Condivisione degli abbonamenti in un'organizzazione

Quando ti iscrivi a prodotti inMarketplace AWS, viene creato un contratto che ti concede una licenza per utilizzare tali prodotti. Se sei membro di un'organizzazione, puoi condividere quella licenza per Amazon Machine Image (AMI), container, machine learning e prodotti di dati con gli altri account di quell'organizzazione. Account AWS È necessario configurare il supporto per le licenze inMarketplace AWS e quindi condividerlo dall'internoAWS License Manager.

Note

Per ulteriori informazioni su AWS Organizations, consulta la [Guida per l'utente di AWS Organizations](#).

Per ulteriori informazioni sulla condivisione delle licenze con l'organizzazione inAWS License Manager, vedere [Licenze concesse](#) nella Guida per l'AWS License Managerutente.

Nel seguente video viene fornita una panoramica dell'esperienza di condivisione delle licenze.

[Distribuisce i diritti diMarketplace AWS licenza \(3:56\)](#)

Gli argomenti seguenti descrivono il processo di visualizzazione, condivisione e tracciamento delle licenze tra gli account.

Argomenti

- [Prerequisiti per la condivisione delle licenze](#)
- [Visualizzazione delle licenze](#)
- [Condivisione delle licenze](#)
- [Monitoraggio dell'uso della licenza](#)

Prerequisiti per la condivisione delle licenze

Prima di poter condividere le licenze,Marketplace AWS devi configurare la condivisione delle licenze per la tua organizzazione. Completa i seguenti processi per configurare la condivisione delle licenze per l'organizzazione:

- Marketplace AWS autorizza la gestione delle licenze per tuo conto in modo che possa creare le relative concessioni di licenza quando acquisti o condividi le licenze. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per condividere i diritti per Marketplace AWS](#).
- Configurare AWS License Manager per il primo utilizzo. Per ulteriori informazioni, vedere Guida [introduttiva AWS License Manager](#) nella Guida per l'AWS License Manager utente.

Visualizzazione delle licenze

Marketplace AWS crea automaticamente licenze per AMI, container, machine learning, software as a service (SaaS) e prodotti di dati acquistati. Puoi condividere tali licenze con altri account nell'organizzazione.

Note

Sebbene le licenze siano create per prodotti SaaS, la condivisione delle licenze SaaS non è attualmente supportata.

Gestisci e condividi le licenze utilizzando AWS License Manager. Tuttavia, puoi utilizzare Marketplace AWS per visualizzare le licenze dei prodotti acquistati dall'interno Marketplace AWS.

Per visualizzare le licenze per i prodotti sottoscritti in Marketplace AWS

1. Accedi [Marketplace AWS](#), accedi e scegli Gestisci abbonamenti.
2. Puoi visualizzare tutte le licenze o visualizzare la licenza per un abbonamento specifico.
 - Per visualizzare tutte le licenze
 - Dal menu Azioni, selezionare Visualizza licenze per visualizzare tutte le licenze Marketplace AWS gestite nella console di License Manager.
 - Per visualizzare le licenze per un singolo abbonamento
 - a. Scegli la scheda del prodotto di cui desideri visualizzarne i dettagli.
 - b. Dal menu Azioni, selezionare Visualizza licenza per visualizzare la licenza per quel prodotto nella console di License Manager.

Note

Puoi anche visualizzare le licenze concesse di cui sono state aggregate di tutti gli account nell'organizzazione. Per ulteriori informazioni, consulta [Licenze concesse](#) nella Guida per l'utente di AWS License Manager.

Condivisione delle licenze

Solo i prodotti AMI, container, machine learning e dati dispongono di licenze che possono essere condivise.

Gli abbonamenti Marketplace AWS hanno un livello di accesso indicato nei dettagli del prodotto:

- I prodotti con un livello di contratto dispongono di una licenza che puoi utilizzare e condividere con altri account dell'organizzazione.
- I prodotti con un livello Entitlement sono licenze che sono state condivise con il tuo account: puoi utilizzare questi prodotti, ma non puoi dividerli.

Marketplace AWS supporta le sovvenzioni, che condividono l'uso di una licenza direttamente con AWS Organizations Account AWS, o un'unità organizzativa che utilizza AWS License Manager. Il processo di attivazione delle sovvenzioni ora include opzioni aggiuntive per sostituire le sovvenzioni attivate per lo stesso prodotto da cui proviene Marketplace AWS. Per ulteriori informazioni, consulta [Licenze concesse](#) nella Guida per l'utente di AWS License Manager.

Note

Per i prodotti che sono limitati a uno specifico Regione AWS, un account con cui condividi la licenza può attivare la licenza solo se l'account si trova in una regione consentita.

Monitoraggio dell'uso della licenza

Puoi tenere traccia delle metriche di licenza basate sull'utilizzo per i prodotti AMI AWS License Manager selezionando la scheda dashboard di utilizzo in ogni rispettiva licenza.

Per ulteriori informazioni sull'utilizzo di License Manager per tenere traccia dell'utilizzo delle licenze, vedere [Licenze concesse](#) nella Guida per l'AWS License Manager utente.

Notifiche agli acquirenti per Marketplace AWS gli eventi

Marketplace AWS fornisce notifiche tempestive tramite e-mail, EventBridge eventi Amazon e argomenti di Amazon Simple Notification Service (Amazon SNS).

Argomenti

- [Notifiche e-mail per Marketplace AWS eventi](#)
- [EventBridge Notifiche Amazon per Marketplace AWS eventi](#)

Notifiche e-mail per Marketplace AWS eventi

In qualità di acquirente Marketplace AWS, ricevi una notifica via email quando si verifica una delle seguenti condizioni:

- Accetti un'offerta.
- Un venditore pubblica una nuova offerta privata correlata all'offerta privata che hai accettato in precedenza o pubblica un aggiornamento dell'offerta precedentemente accettata.

Note

Le notifiche vengono inviate all'indirizzo e-mail associato all'ID acquirente Account AWS.

EventBridge Notifiche Amazon per Marketplace AWS eventi

Marketplace AWS è integrato con Amazon EventBridge, precedentemente chiamato Amazon CloudWatch Events. EventBridge è un servizio di bus di eventi che puoi utilizzare per connettere le tue applicazioni con dati provenienti da diverse fonti. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

In qualità di acquirente, ricevi un evento Marketplace AWS ogni volta che un venditore crea un'offerta e la rende disponibile per l'acquisto. L'evento contiene dettagli come l'ID, la data di scadenza, i dettagli del prodotto e il nome del venditore.

Argomenti

- [Marketplace AWS EventBridge Eventi Amazon dell'API Discovery](#)

Marketplace AWS EventBridge Eventi Amazon dell'API Discovery

Questo argomento fornisce informazioni dettagliate su ogni evento elencato nella tabella seguente.

Azione del venditore	Evento ricevuto dall'acquirente	Argomento correlato
Crea un'offerta e la rende disponibile per l'acquisto	Listing Available	the section called “Eventi per nuove inserzioni”

Eventi per nuove inserzioni

Quando un venditore crea un'offerta e la rende disponibile per l'acquisto, l'acquirente riceve un evento con il seguente tipo di dettaglio: Listing Available.

Note

Per informazioni sulla creazione di EventBridge regole, consulta [EventBridge le regole di Amazon](#) nella Amazon EventBridge User Guide.

Di seguito è riportato un esempio di corpo di evento per un Listing Available evento.

```
{
  "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"
  }
}
```

Integrazione Marketplace AWS con i sistemi di approvvigionamento

Puoi configurare l'integrazione Marketplace AWS e il tuo software di approvvigionamento Coupa o SAP Ariba. Dopo aver completato la configurazione, gli utenti dell'organizzazione possono utilizzare il software di approvvigionamento per cercare e richiedere un abbonamento ai Marketplace AWS prodotti. Dopo l'approvazione della richiesta di abbonamento, la transazione viene completata e l'utente viene informato che l'abbonamento al software è disponibile. Quando l'utente accede a Marketplace AWS, il prodotto software viene elencato come abbonamento acquistato ed è disponibile per l'uso. L'integrazione con il tuo sistema di approvvigionamento può anche integrare le tue Marketplace AWS fatture con il tuo sistema di ordini di acquisto.

Come funziona l'integrazione degli approvvigionamenti

È possibile configurare il software di approvvigionamento da integrare con il Marketplace AWS seguente protocollo commerce extensible markup language (cXML). Questa integrazione crea un punto di accesso nel catalogo di una terza parte, noto come punchout.

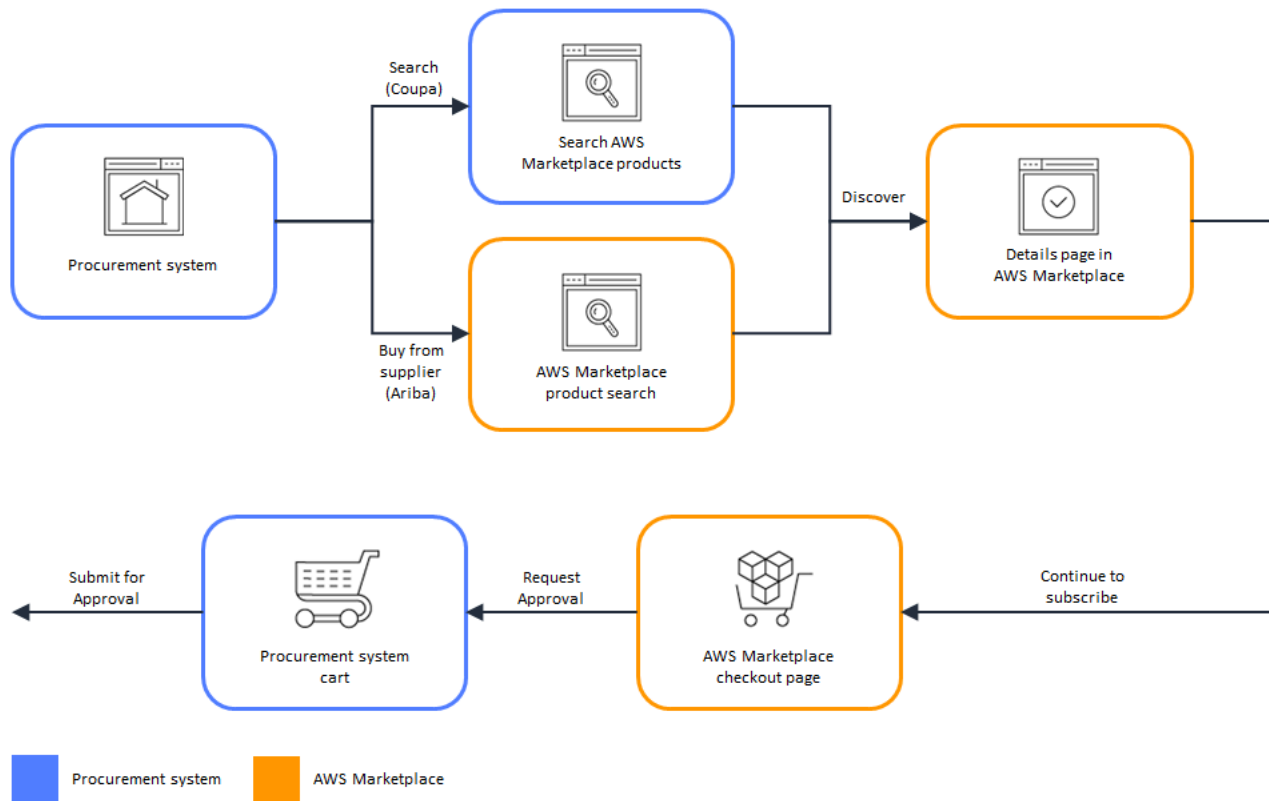
L'integrazione differisce leggermente, in base al sistema di approvvigionamento:

- **Coupa:** utilizzando la funzione Coupa Open Buy, puoi effettuare ricerche all'interno Marketplace AWS di Coupa. Coupa visualizza i risultati della ricerca e, quando l'utente sceglie un prodotto, viene reindirizzato Marketplace AWS a per visualizzare i dettagli. In alternativa, gli utenti del software di approvvigionamento di Coupa possono accedere al Marketplace AWS catalogo nella sezione Shop Online della loro home page. L'utente può anche scegliere di iniziare direttamente Marketplace AWS a cercare i prodotti.
- **SAP Ariba:** Ariba reindirizza gli utenti alla ricerca di software e Marketplace AWS alla ricerca di dettagli su un prodotto. Dopo che un amministratore ha configurato l'integrazione Punchout, gli utenti del software di approvvigionamento di Ariba possono trovare Marketplace AWS il software scegliendo la scheda Catalogo e quindi selezionando il catalogo. Marketplace AWS Questo li reindirizza Marketplace AWS alla ricerca dei prodotti a cui sono interessati.

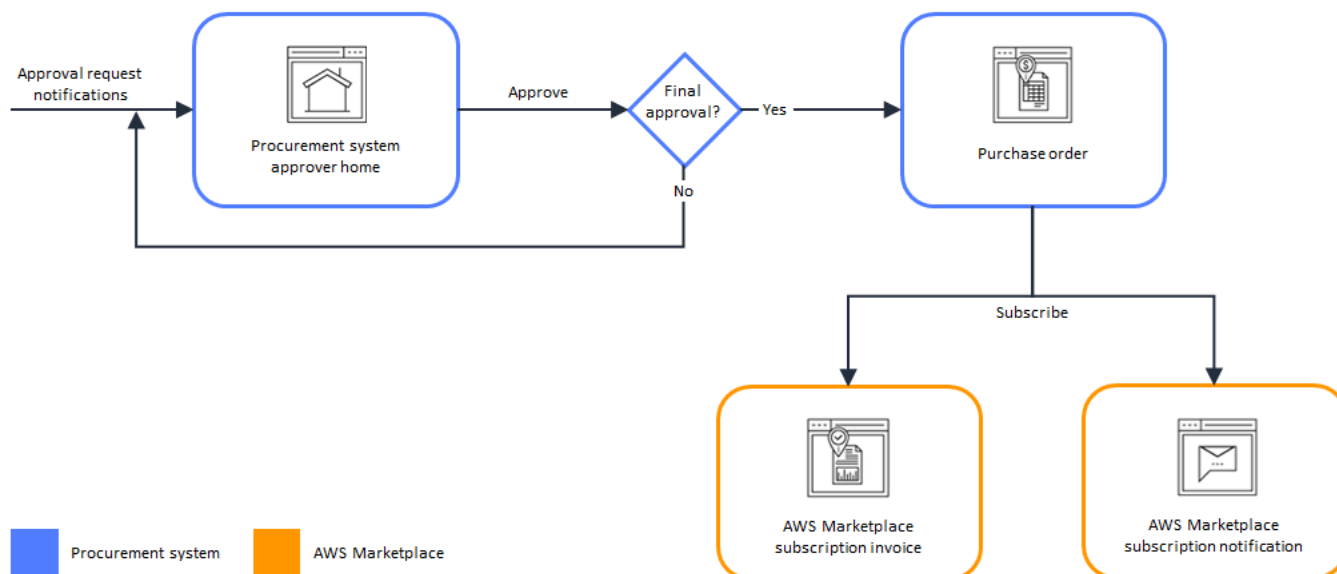
Gli utenti di Ariba devono avviare l'acquisto dall'interno di Ariba, non. Marketplace AWS

Quando l'utente desidera acquistare un abbonamento in cui sta navigando Marketplace AWS, crea una richiesta di iscrizione all'interno Marketplace AWS. Nella pagina di abbonamento del

prodotto, invece di completare l'acquisto, l'utente richiede l'approvazione. La richiesta viene rinviata a un carrello della spesa nel sistema di approvvigionamento per completare il processo di approvazione. Il diagramma seguente mostra il processo per una richiesta di iscrizione al sistema di approvvigionamento.



Quando il sistema di approvvigionamento riceve la richiesta da Marketplace AWS, avvia un flusso di lavoro per completare il processo di approvazione. Dopo l'approvazione della richiesta, il sistema di ordini di acquisto del sistema di approvvigionamento completa automaticamente la transazione Marketplace AWS e notifica all'utente che l'abbonamento è pronto per l'implementazione. Non è necessario che il richiedente effettui la restituzione Marketplace AWS per completare l'acquisto. Tuttavia, potrebbero voler tornare a questa Marketplace AWS pagina per ricevere istruzioni su come utilizzare il prodotto acquistato. Marketplace AWS invia un messaggio di posta elettronica all'AWS account utilizzato per l'accesso Marketplace AWS. Il messaggio e-mail informa il destinatario che l'abbonamento è stato completato e che il software è disponibile tramite Marketplace AWS. Il diagramma seguente mostra il processo di approvazione di una richiesta di iscrizione al sistema di approvvigionamento.



Le note aggiuntive sull'integrazione con i sistemi di approvvigionamento includono quanto segue:

- Le versioni di prova gratuite non generano una fattura nel sistema di approvvigionamento, poiché non comportano alcun addebito.
- I contratti che prevedono un addebito una tantum in aggiunta agli pay-as-you-go addebiti possono richiedere due serie di approvazioni. Un'approvazione riguarda il prezzo del contratto (o annuale) e l'altra il prezzo orario o unitario (pay-as-you-go).
- I clienti con PSI (Procurement System Integrations) possono attivare le preapprovazioni per prodotti gratuiti e prodotti BYOL. Sono disponibili due impostazioni, una per Free e una per BYOL. Quando l'impostazione è abilitata, gli ordini vengono preapprovati in Marketplace AWS e i clienti non devono inviare gli ordini al proprio sistema di approvvigionamento per l'approvazione. Quando l'impostazione è disabilitata, i clienti invieranno le approvazioni tramite il pulsante Richiedi approvazione al proprio sistema di approvvigionamento. Quando l'impostazione di preapprovazione per i prodotti Free e BYOL è disabilitata, gli ordini da 0,00 USD vengono prodotti nel sistema di approvvigionamento del cliente. Per ulteriori informazioni sulle integrazioni dei sistemi di approvvigionamento, vedere <https://aws.amazon.com/marketplace/features/procurementsystem>

Configurazione dell'integrazione del sistema di approvvigionamento

Per configurare l'integrazione tra il sistema di approvvigionamento Marketplace AWS e il sistema di approvvigionamento, è necessario avviare il processo Marketplace AWS e completarlo nel sistema di approvvigionamento. Le informazioni generate in vengono utilizzate Marketplace AWS

per configurare il punchout del sistema di approvvigionamento. Per completare la configurazione, gli account utilizzati devono soddisfare i seguenti requisiti:

- L'utente Account AWS utilizzato per completare la Marketplace AWS configurazione deve essere l'account di gestione e disporre delle autorizzazioni AWS Identity and Access Management (IAM) definite nella policy `AWSMarketplaceProcurementSystemAdminFullAccess` gestita.
- L'account del sistema di approvvigionamento utilizzato per completare la configurazione deve disporre dell'accesso amministrativo per configurare un contratto, un fornitore e un catalogo di punchout nel sistema di approvvigionamento.

Configurazione delle autorizzazioni IAM

Le seguenti autorizzazioni IAM si trovano nella policy [AWSpolitica gestita: AWSMarketplaceProcurementSystemAdminFullAccess](#) gestita e sono necessarie per configurare l'integrazione tra un sistema di approvvigionamento Marketplace AWS e un sistema di approvvigionamento.

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

Ti consigliamo di utilizzare le autorizzazioni gestite da IAM anziché configurare manualmente le autorizzazioni. L'utilizzo di questo approccio è meno soggetto a errori umani e, se le autorizzazioni cambiano, la politica gestita viene aggiornata. Per ulteriori informazioni sulla configurazione e l'utilizzo di IAM in Marketplace AWS, vedere [Sicurezza attiva Marketplace AWS](#).

Configurazione Marketplace AWS per l'integrazione con Coupa

Dopo aver impostato le autorizzazioni IAM, sei pronto per configurare Marketplace AWS l'integrazione con Coupa. Accedere a Gestire l'approvvigionamento. Nel riquadro Gestisci i sistemi di approvvigionamento, inserisci un nome e una descrizione per il punchout. Puoi anche passare l'integrazione alla modalità di test in modo che gli utenti possano testare l'integrazione senza creare abbonamenti ai prodotti finché non sei pronto. Per configurare la Marketplace AWS parte dell'integrazione, completa la procedura seguente.

Da configurare Marketplace AWS per l'integrazione con Coupa

1. Da [Marketplace AWS Manage Procurement Systems](#), in Sistemi di approvvigionamento, scegli Configura l'integrazione Coupa.
2. Nella pagina Gestisci l'integrazione di Coupa, in Informazioni sull'account, inserisci il nome e la descrizione della tua integrazione.

Note

È possibile che le fatture nella AWS Billing console facciano riferimento all'ordine di acquisto del commerce extensible markup language (cXML) utilizzato per sottoscrivere il prodotto contrattuale Software as a Service (SaaS). In tal caso, puoi abilitare l'integrazione della fatturazione utilizzando un ruolo collegato al servizio nelle impostazioni. Marketplace AWS

3. È possibile attivare o disattivare le impostazioni di configurazione per Abilita il reindirizzamento e la modalità Test, quindi selezionare Salva per completare l'integrazione nel Marketplace AWS sistema.

Dopo aver completato l'integrazione in Marketplace AWS, è necessario procedere alla configurazione dell'integrazione in Coupa. Utilizzi le informazioni generate in questa pagina per configurare il punchout nel tuo sistema Coupa.

La Marketplace AWS configurazione predefinita è che la modalità di test sia abilitata. In modalità test, le richieste di abbonamento vanno al backend Coupa in modo da poter vedere l'intero flusso, ma non viene creata una fattura finale. Ciò consente di completare la configurazione e abilitare il punchout in modo pianificato.

Note

Puoi attivare o disattivare la modalità di test, se necessario.

Non dimenticare di disattivare la modalità di test al termine dell'integrazione. In caso contrario, sembrerà che gli utenti del sistema stiano creando richieste, ma non verrà acquistato alcun software.

Configurazione di Coupa

Per configurare l'integrazione con Marketplace AWS il tuo sistema Coupa, copia le informazioni dal riquadro Informazioni sull'acquisto della pagina di integrazione Gestisci Coupa in Marketplace AWS. Utilizza queste informazioni per completare i passaggi nei seguenti link che ti guidano nella configurazione del tuo sistema di approvvigionamento Coupa:

- [Configurazione Coupa Punchout](#)
- [Configurazione di un fornitore per gli ordini di acquisto cXML](#)

Note

Per informazioni sui codici UNSPSC utilizzati da Marketplace AWS, vedere [Codici UNSPSC utilizzati da Marketplace AWS](#)

Configurazione Marketplace AWS per l'integrazione con SAP Ariba

Marketplace AWS Per configurare l'integrazione con Ariba, è necessario collaborare con il team Marketplace AWS operativo per creare un punchout di livello 1. Per ulteriori informazioni su SAP Ariba punchout, vedere [Introduzione a SAP Ariba PunchOut sul sito Web della community SAP](#).

Raccogli le seguenti informazioni per prepararti alla configurazione della configurazione:

- Il tuo ID account Account AWS. Se fai Account AWS parte di un'AWS organizzazione, ti serve anche l'ID dell'account di gestione.
- L'ID di rete Ariba (ANID) per il tuo sistema SAP Ariba.

Note

Per informazioni sugli ANID in Ariba e per le risposte ad altre domande su Ariba, consulta la pagina [Ariba Network for Suppliers: Frequently Asked Questions](#) sul sito web di SAP Ariba.

Da configurare Marketplace AWS per l'integrazione con Ariba

1. Da [Marketplace AWS Manage Procurement Systems, in Sistemi](#) di approvvigionamento, scegli Configura l'integrazione con Ariba.
2. Nella pagina Gestisci l'integrazione di SAP Ariba, in Informazioni sull'account, inserisci il nome e la descrizione dell'integrazione, nonché il SAP Ariba Network ID (ANID) per il tuo sistema Ariba.

Note

È possibile che le fatture nella AWS Billing console facciano riferimento all'ordine di acquisto cXML utilizzato per sottoscrivere il prodotto contrattuale SaaS. In tal caso, puoi abilitare l'integrazione della fatturazione utilizzando un ruolo collegato al servizio nelle impostazioni. Marketplace AWS

3. Assicurati che la modalità Test sia abilitata, quindi seleziona Salva per salvare le impostazioni di Marketplace AWS integrazione.
4. [Contattaci](#) per avviare il processo di creazione della tua integrazione SAP Ariba. Includi le informazioni di cui sopra. Marketplace AWS ti invia le istruzioni per configurare e testare l'integrazione con Ariba.

Note

È necessario disporre dell'accesso amministratore al sistema SAP Ariba per creare il rapporto con il fornitore. Marketplace AWS

Seguendo le istruzioni e le impostazioni di configurazione del Marketplace AWS team, crei l'integrazione nel tuo ambiente di test SAP Ariba, con Marketplace AWS esecuzione in modalità test. Nell'ambiente di test, le richieste di abbonamento vengono inviate al backend di Ariba in modo

da poter visualizzare il flusso completo, comprese le approvazioni, senza creare un abbonamento e non viene generata alcuna fattura. Marketplace AWS Questo approccio consente di testare la configurazione prima di abilitare il punchout in produzione. Una volta completati i test e pronti per passare alla produzione, [contattaci](#) per configurare l'account nell'ambiente di produzione.

Note

Non dimenticare di passare alla produzione quando hai finito di testare la tua integrazione. In caso contrario, gli utenti del sistema crederanno che stiano creando richieste, ma non verrà acquistato alcun software.

Una volta completati i test e dopo aver collaborato con il Marketplace AWS team per disattivare la modalità test, l'integrazione è completa.

Per ulteriori informazioni sulla configurazione di SAP Ariba, consulta i seguenti argomenti di SAP Ariba:

- [SAP Ariba PunchOut](#) sul sito web di SAP Ariba
- [Introduzione a SAP Ariba PunchOut](#) sul sito web della community SAP

Note

Per informazioni sui codici UNSPSC utilizzati da Marketplace AWS, vedere. [Codici UNSPSC utilizzati da Marketplace AWS](#)

Codici UNSPSC utilizzati da Marketplace AWS

Marketplace AWS utilizza il seguente codice UNSPSC (United Nations Standard Products and Services) per le offerte di software che vengono rispedito al carrello di approvvigionamento:
43232701

Disattivazione dell'integrazione del sistema di approvvigionamento

Per disabilitare l'integrazione con Coupa o SAP Ariba, è necessario rimuovere l'integrazione punchout dall'interno del sistema di approvvigionamento. Per fare ciò, disabilita la funzionalità

di reindirizzamento automatico Marketplace AWS dall'interno di Coupa o Ariba. Ciò disabilita l'integrazione, ma mantiene le impostazioni e consente di riattivarla facilmente.

Se è necessario rimuovere completamente la configurazione di integrazione sul Marketplace AWS lato, è necessario [contattarci](#).

Prove libere

Alcuni prodotti elencati Marketplace AWS offrono prove gratuite. La versione di prova gratuita consente di provare il software prima di acquistarlo. Le prove gratuite sono limitate a un determinato periodo di utilizzo gratuito o per un periodo di tempo specifico. Non puoi sospendere un periodo di prova gratuito una volta iniziato.

Prezzi del software e dell'infrastruttura

Le prove gratuite offerte dai venditori si applicano solo ai prezzi del software del prodotto indicato su Marketplace AWS. Gli acquirenti sono responsabili di tutti i costi di infrastruttura durante l'utilizzo del prodotto del venditore, Marketplace AWS indipendentemente dal fatto che il prezzo del software includa una prova gratuita. Questi costi di infrastruttura sono stabiliti da AWS e sono disponibili nelle rispettive pagine dei prezzi. Ad esempio, se ti abboni a un prodotto Amazon Machine Image (AMI) con una prova gratuita, non ti verrà addebitato alcun costo per l'utilizzo dell'AMI durante la prova gratuita. Tuttavia, è possibile che ti venga addebitata una tariffa per l'istanza Amazon EC2 su cui si esegue il prodotto AMI.

Note

Alcuni prodotti potrebbero richiedere un'AWS infrastruttura aggiuntiva per funzionare. Ad esempio, i venditori potrebbero fornire istruzioni o modelli di distribuzione che implementano sistemi di bilanciamento del carico, storage, database o altro Servizi AWS nel tuo Account AWS. Per capire cosa ha richiesto Servizi AWS il venditore per il suo prodotto, consulta le pagine di dettaglio dei prodotti in cui sono elencati Marketplace AWS. Quindi, consulta le pagine dei prezzi di questi Servizi AWS.

Prove gratuite per prodotti basati su AMI

Alcuni prodotti AMI con tariffa oraria o oraria con tariffa annuale Marketplace AWS sono disponibili in versione di prova gratuita. Quando ti iscrivi a una prova gratuita, puoi eseguire un'istanza Amazon EC2 del prodotto AMI per una durata stabilita dal venditore senza incorrere nei costi orari del software. Sei responsabile della tariffa di infrastruttura. L'avvio di istanze Amazon EC2 aggiuntive comporterà l'addebito orario del software per istanza. Le versioni di prova gratuite vengono convertite automaticamente in un abbonamento a pagamento alla scadenza.

Se non interrompi l'istanza Amazon EC2 prima della fine della prova gratuita, al termine della prova gratuita ti verranno addebitati costi orari per il software. L'annullamento dell'iscrizione alla versione di prova gratuita non comporta la chiusura automatica delle istanze Amazon EC2 e comporta l'addebito di costi software per l'uso continuato. Per ulteriori informazioni sui prezzi relativi all'infrastruttura, consulta [Prezzi di Amazon EC2](#).

Prove gratuite per prodotti a base di contenitori

Alcuni prodotti in container con tariffa oraria o oraria con prezzi a lungo termine Marketplace AWS sono disponibili versioni di prova gratuite. Quando ti iscrivi a una prova gratuita, puoi eseguire diverse attività di Elastic Container Service (Amazon ECS) o dei pod di Amazon Elastic Kubernetes Service (Amazon EKS) per una durata senza incorrere in tariffe orarie per il software. Il numero di attività o di pod inclusi e la durata della prova gratuita sono stabiliti dal venditore. Sei responsabile della tariffa di infrastruttura. L'avvio di attività o pod aggiuntivi oltre al numero incluso nella versione di prova gratuita comporterà l'addebito orario del software per attività o pod. Le versioni di prova gratuite vengono convertite automaticamente in un abbonamento a pagamento alla scadenza.

Se non interrompi l'attività o il pod prima della fine della prova gratuita, al termine della prova gratuita verranno addebitati costi orari del software. L'annullamento della sottoscrizione alla versione di prova gratuita non pone fine automaticamente alle attività o ai pod e comporta l'addebito di costi software per qualsiasi uso continuato. Per ulteriori informazioni sui costi dell'infrastruttura, consulta [i prezzi di Amazon ECS](#) e [Amazon EKS](#).

Prove libere di prodotti di machine learning

Alcuni prodotti di machine learning con prezzi orari Marketplace AWS sono disponibili in versione di prova gratuita. Quando ti iscrivi a una versione di prova gratuita, puoi eseguire Amazon SageMaker endpoint, processi di trasformazione in batch o processi di formazione per una durata stabilita dal venditore senza incorrere nei costi orari del software. Sei responsabile della tariffa di infrastruttura. Le versioni di prova gratuite vengono convertite automaticamente in un abbonamento a pagamento alla scadenza.

Se non interrompi alcun SageMaker endpoint Amazon, un processo di trasformazione in batch o un processo di formazione prima della fine della prova gratuita, al termine della prova gratuita ti verranno addebitati costi orari per il software. L'annullamento dell'iscrizione alla versione di prova gratuita non pone fine automaticamente ai tuoi SageMaker endpoint Amazon, ai processi di trasformazione in batch o ai lavori di formazione e ti verranno addebitati costi del software per qualsiasi uso continuato. Per ulteriori informazioni sui costi dell'infrastruttura, consulta [i SageMaker prezzi di Amazon](#).

Prove gratuite per prodotti SaaS

I prodotti Software as a Service (SaaS) Marketplace AWS sono disponibili in versione di prova gratuita. Le versioni di prova gratuite di SaaS non si convertono automaticamente in contratti a pagamento. Se non desideri più la prova gratuita, puoi lasciarla scadere. Per ulteriori informazioni, consultare [Versioni di prova gratuite SaaS](#).

Utilizzo del piano di utilizzo gratuito AWS con AWS Marketplace

Per aiutare i nuovi Amazon Web Services (AWS) i clienti iniziano a utilizzare il cloud, AWS ha introdotto un piano di utilizzo gratuito. Il piano gratuito può essere utilizzato per tutto ciò che desideri eseguire nel cloud: avviare nuove applicazioni, testare applicazioni esistenti nel cloud o semplicemente acquisire esperienza pratica con AWS. Alla scadenza del periodo di utilizzo gratuito (o se l'utilizzo dell'applicazione supera i limiti del piano di utilizzo gratuito), si paga semplicemente lo standard, pay-as-you-go tariffe di servizio. Per ulteriori informazioni, consulta [Piano gratuito di AWS](#).

I clienti del piano gratuito di AWS possono utilizzare il software gratuito AWS Marketplace per un massimo di 750 ore di utilizzo di Amazon Elastic Compute Cloud (Amazon EC2) ogni mese per un anno. Per iniziare, consulta [AWS Marketplace](#).

Aggiungere abbonamenti AWS Marketplace ad AWS Service Catalog

Service Catalog consente alle organizzazioni di creare e gestire cataloghi di servizi IT approvati per l'uso su Amazon Web Services (AWS). Questi servizi IT includono soluzioni di vario tipo, da immagini di macchine virtuali, server, software, database a architetture di applicazioni multi-tier complete.

Service Catalog consente di gestire centralmente i servizi IT distribuiti di frequente. Service Catalog ti aiuta a raggiungere una governance coerente e a soddisfare i requisiti di conformità, consentendo al contempo agli utenti di implementare rapidamente solo i servizi IT approvati di cui hanno bisogno.

Per ulteriori informazioni, vedere [AggiungereMarketplace AWS prodotti al portafoglio](#) nella Service Catalog Administrator Guide.

Recensioni di prodotti

Marketplace AWS desidera che gli acquirenti ottengano le informazioni di cui hanno bisogno per fare scelte di acquisto intelligenti. In qualità di cliente AWS, puoi inviare recensioni scritte per gli articoli elencati in Marketplace AWS. Ti invitiamo a condividere le tue opinioni, sia favorevoli che sfavorevoli.

Note

I prodotti dati non supportano le recensioni dei prodotti.

Linee guida

Chiunque abbia un Marketplace AWS l'abbonamento a un prodotto può creare una recensione. Utilizza le seguenti linee guida per scrivere recensioni di prodotti:

- **Includi i motivi**— Le migliori recensioni includono non solo se un prodotto ti è piaciuto o non ti è piaciuto, ma anche perché. Puoi parlare di prodotti correlati e di come questo articolo si confronta con essi.
- **Sii specifico**— Concentrati sulle caratteristiche specifiche del prodotto e sulla tua esperienza con esso. Per le recensioni dei video, scrivi una breve introduzione.
- **Sii conciso**— Le recensioni scritte devono contenere almeno 20 parole e sono limitate a 5.000 parole. La lunghezza ideale è di 75-500 parole.
- **Sii sincero**— La tua opinione onesta sul prodotto, positiva o negativa, è apprezzata. Informazioni utili possono influenzare le decisioni di acquisto dei nostri clienti.
- **Sii trasparente**— Se hai ricevuto un prodotto gratuito in cambio della tua recensione, comunicalo in modo chiaro e ben visibile.

Restrizioni

AWS si riserva il diritto di rimuovere le recensioni che includono uno dei seguenti contenuti.

- Materiale oggettivo, tra cui:
 - Contenuti osceni o di cattivo gusto
 - Osservazioni volgari o dispettose

- Promozione di comportamenti illegali o immorali
- Contenuti promozionali, tra cui:
 - Pubblicità, materiale promozionale o post ripetuti che sottolineano lo stesso punto
 - Sentimenti di o per conto di una persona o di un'azienda con un interesse finanziario nel prodotto o in un prodotto direttamente concorrente (comprese le recensioni di autori, editori, produttori o commercianti terzi che vendono il prodotto)
 - Recensioni scritte per qualsiasi forma di compensazione diversa da una copia gratuita del prodotto, comprese le recensioni che fanno parte di un pacchetto pubblicitario a pagamento
 - Recensioni scritte da un cliente senza un abbonamento verificabile al prodotto
- Contenuti inappropriati, tra cui:
 - Contenuti copiati da altri, incluse citazioni eccessive
 - Informazioni di contatto o URL esterni ad Amazon.com
 - Dettagli sulla disponibilità o sull'ordinazione/spedizione alternativa
 - Video con filigrane
 - Commenti su altre recensioni visibili sulla pagina, poiché la visibilità della pagina è soggetta a modifiche senza preavviso
 - Contenuti in lingua straniera, a meno che non vi sia una connessione chiara al prodotto
 - Testo con problemi di formattazione
- Informazioni fuori tema, tra cui:
 - Feedback sul venditore o sulla tua esperienza di spedizione
 - Feedback su errori di battitura o imprecisioni nel nostro catalogo o nella descrizione del prodotto; utilizza invece il modulo di feedback in fondo alla pagina del prodotto

Per domande sulle recensioni dei clienti, [contattaci](#).

Tempi e aspettative

Ci impegniamo a elaborare le recensioni dei prodotti il più rapidamente possibile. Tuttavia, il Marketplace AWS il team deve comunicare sia con il revisore che con il venditore per confermare ed esaminare la validità del feedback rispetto al nostro [the section called "Linee guida"](#) e [the section called "Restrizioni"](#). Seguiamo lo stesso [tempistica e aspettative](#) guida descritta nel Marketplace AWS Guida del venditore quanto tempo ci vorrà per completare il processo.

Ottenere supporto

Per uso generale Marketplace AWS Problemi relativi a [contattaci](#). Per domande sul software acquistato tramite Marketplace AWS, contatta il venditore del software.

Marketplace AWS Vendor Insights

Marketplace AWS Vendor Insights semplifica la valutazione dei rischi del software aiutandoti a procurarti software di cui ti fidi e che soddisfino gli standard del tuo settore. Con Marketplace AWS Vendor Insights, puoi monitorare il profilo di sicurezza di un prodotto quasi in tempo reale da un'unica interfaccia utente. Riduce lo sforzo di valutazione fornendo una dashboard delle informazioni sulla sicurezza di un prodotto software. È possibile utilizzare la dashboard per visualizzare e valutare informazioni, come la privacy dei dati, la sicurezza delle applicazioni e il controllo degli accessi.

Marketplace AWS Vendor Insights raccoglie i dati sulla sicurezza dai venditori e supporta gli acquirenti acquistando software affidabili che soddisfino continuamente gli standard del settore. Grazie all'integrazione con AWS Audit Manager, Marketplace AWS Vendor Insights può inserire automaticamente le informazioni up-to-date di sicurezza per i tuoi prodotti Software as a Service (SaaS). Marketplace AWS Marketplace AWS Vendor Insights si integra con i report AWS Artifact di terze parti in modo da poter accedere ai report di conformità su richiesta per il software del fornitore, oltre ai report per Servizi AWS.

Marketplace AWS Vendor Insights fornisce informazioni basate su prove relative a 10 categorie di controllo e controlli multipli. Raccoglie le informazioni basate sull'evidenza da tre fonti:

- Account di produzione del fornitore: tra i molteplici controlli, 25 controlli supportano la raccolta di prove in tempo reale dagli account di produzione del fornitore. Le prove in tempo reale per ogni controllo sono generate da una o più AWS Config regole che valutano le impostazioni di configurazione delle risorse di un venditore. AWS Le prove in tempo reale sono il metodo per aggiornare costantemente i dati provenienti da più fonti per presentare le informazioni più aggiornate. AWS Audit Manager acquisisce le prove e le invia alla dashboard di Marketplace AWS Vendor Insights.
- Rapporti ISO 27001 e SOC 2 Type II del fornitore: le categorie di controllo sono mappate ai controlli contenuti nei rapporti dell'International Organization for Standardization (ISO) e Service Organization Control (SOC) 2. Quando i venditori condividono questi report con Marketplace AWS Vendor Insights, il servizio estrae i dati pertinenti e li presenta nella dashboard.
- Autovalutazione del fornitore: i venditori completano un'autovalutazione. Possono anche creare e caricare altri tipi di autovalutazione, tra cui l'autovalutazione della sicurezza di Marketplace AWS Vendor Insights e il Consensus Assessment Initiative Questionnaire (CAIQ).

Il video seguente mostra come semplificare la valutazione del rischio SaaS e Marketplace AWS utilizzando Vendor Insights.

Guida introduttiva a Marketplace AWS Vendor Insights come acquirente

Marketplace AWS Vendor Insights presenta informazioni sulla sicurezza per i prodotti software disponibili in Marketplace AWS. È possibile utilizzare Marketplace AWS Vendor Insights per visualizzare i profili di sicurezza per i prodotti in Marketplace AWS.

La dashboard di Marketplace AWS Vendor Insights presenta gli elementi di conformità e le informazioni sul controllo di sicurezza per un prodotto software che utilizza Marketplace AWS Vendor Insights per valutare il prodotto. Marketplace AWS Vendor Insights raccoglie le informazioni basate sull'evidenza per i molteplici controlli di sicurezza presentati nella dashboard.

L'utilizzo di Marketplace AWS Vendor Insights per accedere alle informazioni di sicurezza e conformità dei prodotti è gratuito.

Trova prodotti con Marketplace AWS Vendor Insights

Puoi visualizzare il profilo e le informazioni di riepilogo di un prodotto nella dashboard di Marketplace AWS Vendor Insights o selezionare i controlli della categoria e saperne di più sui dati raccolti sul prodotto. Per trovare prodotti in Marketplace AWS Marketplace AWS Vendor Insights, utilizza la procedura seguente.

Per trovare prodotti con Marketplace AWS Vendor Insights

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Scegli Visualizza tutti i prodotti.
3. Visualizza i prodotti con il tag Vendor Insights.
4. In Perfeziona i risultati per Vendor Insights, scegli Profili di sicurezza.
5. Dalla pagina dei dettagli del prodotto, in Panoramica del prodotto, scegli la sezione Vendor Insights.
6. Scegli Visualizza tutti i profili per questo prodotto.
7. Puoi visualizzare i dettagli sul prodotto nella Panoramica e un elenco dei certificati di sicurezza ricevuti.

8. Scegli Richiedi accesso.
9. Nella pagina Richiedi accesso ai dati di Vendor Insight, fornisci le tue informazioni, quindi scegli Richiedi accesso.

Viene visualizzato un messaggio di successo che indica che hai richiesto correttamente l'accesso ai dati di Marketplace AWS Vendor Insights per questo prodotto.

Richiedi l'accesso ai dati di valutazione iscrivendoti

Con Marketplace AWS Vendor Insights, puoi monitorare continuamente il profilo di sicurezza del software del fornitore. Innanzitutto, iscriviti o richiedi l'accesso ai dati di valutazione del fornitore per il prodotto che desideri monitorare. Se non desideri più monitorare i dati di valutazione di un prodotto, puoi annullare l'iscrizione ai relativi dati di valutazione. L'utilizzo di Marketplace AWS Vendor Insights per accedere alle informazioni di sicurezza e conformità dei prodotti è gratuito. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di [Marketplace AWS Vendor Insights](#).

Per avere accesso a tutti i dati di valutazione per un prodotto di un fornitore specifico, è necessario abbonarsi ai dati di valutazione del prodotto.

Per abbonarsi ai dati di valutazione di Marketplace AWS Vendor Insights per un prodotto

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Scegli Vendor Insights.
3. Da Vendor Insights, scegli un prodotto.
4. Seleziona la scheda Panoramica.
5. Scegli Richiedi accesso.
6. Inserisci le tue informazioni nei campi forniti.
7. Quando hai finito, scegli Richiedi accesso.

Viene visualizzato un messaggio di successo che indica che hai richiesto l'accesso a tutti i dati di valutazione del fornitore per questo prodotto.

Annulla l'iscrizione ai dati di valutazione

Se non desideri più accedere ai dati di valutazione per un prodotto del fornitore, puoi annullare l'iscrizione ai dati di valutazione del prodotto.

Per annullare l'iscrizione ai dati di valutazione di Marketplace AWS Vendor Insights per un prodotto

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Scegli Vendor Insights.
3. Dalla pagina dei dettagli del prodotto, scegli un prodotto, quindi scegli Annulla iscrizione.
4. Leggi i termini relativi all'annullamento dell'iscrizione ai dati di Marketplace AWS Vendor Insights.
5. Digita **Unsubscribe** nel campo di immissione del testo, quindi scegli Annulla iscrizione.

Viene visualizzato un messaggio di successo, che indica che hai annullato l'iscrizione ai dati di Marketplace AWS Vendor Insights e che non ti verrà più addebitato alcun costo per l'accesso.

Visualizzazione del profilo di sicurezza di un prodotto con Marketplace AWS Vendor Insights

Marketplace AWS Vendor Insights raccoglie dati sulla sicurezza dai venditori. Il profilo di sicurezza di un prodotto mostra informazioni aggiornate sulla sicurezza, la resilienza, la conformità e altri fattori del prodotto necessari per la valutazione. Queste informazioni supportano gli acquirenti come te aiutandoti a procurarsi software affidabile che soddisfi continuamente gli standard del settore. Per ogni prodotto SaaS (Software as a Service) che valuta, Marketplace AWS Vendor Insights raccoglie le informazioni basate sull'evidenza per molteplici controlli di sicurezza.

Argomenti

- [Marketplace AWS Dashboard in Vendor Insights](#)
- [Visualizza il profilo di sicurezza di un prodotto SaaS](#)
- [Comprensione delle categorie di controllo](#)

Marketplace AWS Dashboard in Vendor Insights

La dashboard presenta gli elementi di conformità e le informazioni sul controllo di sicurezza per un prodotto software raccolti da Marketplace AWS Vendor Insights. Vengono fornite informazioni basate su prove per tutte le [categorie di controllo della](#) sicurezza, come la modifica della residenza dei dati o la scadenza della certificazione. Il dashboard consolidato fornisce modifiche alle informazioni sulla conformità. Marketplace AWS Vendor Insights elimina la necessità di creare questionari aggiuntivi e utilizzare software di valutazione del rischio. Con una dashboard costantemente

aggiornata e convalidata, puoi monitorare continuamente il controllo di sicurezza del software dopo l'approvvigionamento.

Visualizza il profilo di sicurezza di un prodotto SaaS

Marketplace AWS Vendor Insights ti aiuta a prendere decisioni sul software di un venditore.

Marketplace AWS Vendor Insights estrae i dati dalle informazioni basate sull'evidenza di un venditore in 10 categorie di controllo e più controlli. Puoi visualizzare il profilo e le informazioni di riepilogo per un prodotto SaaS sulla dashboard o selezionare le categorie di controllo per saperne di più sui dati raccolti. Devi essere abbonato al prodotto e avere accesso per visualizzare le informazioni sulla conformità tramite il profilo.

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Scegli Vendor Insights.
3. Da Vendor Insights, scegli un prodotto.
4. Nella pagina dei dettagli del profilo, scegli la scheda Sicurezza e conformità.

Note

Un numero in un cerchio rosso indica il numero di controlli non conformi.

5. Per le categorie di controllo, scegli il testo sotto una delle categorie elencate per visualizzare ulteriori informazioni.
 - Scegli il primo nome di controllo (disponi di una politica/procedura per garantire la conformità ai requisiti legislativi, normativi e contrattuali applicabili?).
 - Leggi le informazioni presentate. È inoltre possibile visualizzare i report tratti da rapporti AWS Artifact di terze parti o visualizzare le eccezioni del revisore.
 - Seleziona il nome del prodotto nella barra di navigazione in alto per tornare alla pagina dei dettagli del prodotto.

Comprensione delle categorie di controllo

Marketplace AWS Vendor Insights fornisce informazioni basate su prove provenienti da più controlli all'interno di 10 categorie di controllo. Marketplace AWS Vendor Insights raccoglie le informazioni da tre fonti: conti di produzione dei fornitori, autovalutazione dei fornitori e report ISO 27001 e SOC

2 Tipo II dei fornitori. Per ulteriori informazioni su queste fonti, vedere. [Marketplace AWS Vendor Insights](#)

L'elenco seguente fornisce una descrizione di ciascuna categoria di controllo:

Gestione degli accessi

Identifica, traccia, gestisce e controlla l'accesso a un sistema o un'applicazione.

Sicurezza delle applicazioni

Verifica se la sicurezza è stata incorporata nell'applicazione durante la progettazione, lo sviluppo e il test.

Politica di controllo, conformità e sicurezza

Valuta l'aderenza di un'organizzazione ai requisiti normativi.

Resilienza e continuità aziendale

Valuta la capacità dell'organizzazione di adattarsi rapidamente alle interruzioni mantenendo la continuità aziendale.

Sicurezza dei dati

Protegge dati e risorse.

Sicurezza dei dispositivi degli utenti finali

Protegge i dispositivi portatili degli utenti finali e le reti a cui sono connessi da minacce e vulnerabilità.

Risorse umane

Valuta la divisione relativa ai dipendenti per la gestione dei dati sensibili durante processi quali l'assunzione, il pagamento e il licenziamento dei dipendenti.

Sicurezza dell'infrastruttura

Protegge gli asset critici da minacce e vulnerabilità.

Gestione del rischio e risposta agli incidenti

Valuta il livello di rischio ritenuto accettabile e le misure adottate per rispondere a rischi e attacchi.

Politica di sicurezza e configurazione

Valuta le politiche di sicurezza e le configurazioni di sicurezza che proteggono gli asset di un'organizzazione.

Controlla i set di categorie

Le tabelle seguenti forniscono informazioni dettagliate per ogni categoria con informazioni sui valori raccolti per ciascuna categoria. L'elenco seguente descrive il tipo di informazioni all'interno di ogni colonna della tabella:

- **Set di controlli:** i controlli vengono assegnati a un set di controlli e ogni controllo riflette la funzione di sicurezza della relativa categoria. Ogni categoria ha più set di controlli.
- **Nome del controllo:** nome della politica o della procedura. «Richiede un'attestazione manuale» significa che è richiesta la conferma o la documentazione scritta della politica o della procedura.
- **Descrizione del controllo:** domande, informazioni o documentazione necessarie su questa politica o procedura.
- **Dettagli sull'estrazione delle prove:** informazioni e contesto necessari sul controllo per ottenere ulteriormente i dati necessari per questa categoria.
- **Valore del campione:** esempio fornito a titolo indicativo su come potrebbe essere un valore di conformità per questa categoria in modo che sia conforme agli standard normativi.

Argomenti

- [Controlli di gestione degli accessi](#)
- [Controlli di sicurezza delle applicazioni](#)
- [Controlli di audit e conformità](#)
- [Controlli di resilienza aziendale](#)
- [Controlli di sicurezza dei dati](#)
- [Controlli di sicurezza dei dispositivi degli utenti finali](#)
- [Controlli delle risorse umane](#)
- [Controlli di sicurezza dell'infrastruttura](#)
- [Gestione del rischio e controlli della risposta agli incidenti](#)
- [Controlli delle politiche di sicurezza e configurazione](#)

Controlli di gestione degli accessi

I controlli di gestione degli accessi identificano, tracciano, gestiscono e controllano l'accesso a un sistema o un'applicazione. Questa tabella elenca i valori e le descrizioni per i controlli di gestione degli accessi.

Set di controlli	Titolo di controllo	Descrizione del controllo
Autenticazione sicura	Gestione degli accessi 3.1.1 - Autenticazione sicura - Dati personali inseriti UserId (richiede l'attestazione manuale)	Sono necessari dati personali (diversi dall'indirizzo e-mail) nell'ID utente?
	Gestione degli accessi 3.1.2 - Autenticazione sicura - L'applicazione supporta l'autenticazione a due fattori (richiede l'attestazione manuale)	L'applicazione supporta l'autenticazione a due fattori?
	Gestione degli accessi 3.1.3 - Autenticazione sicura - Blocco dell'account (richiede l'attestazione manuale)	L'account del cliente è bloccato se non riusciti?
Gestione delle credenziali	Gestione degli accessi 3.2.1 - Gestione delle credenziali - Politica delle password	L'applicazione ha una politica solida delle password?
	Gestione degli accessi 3.2.2 - Gestione delle credenziali - Crittografia delle password	La politica in materia di password richiede che le credenziali di accesso (password) vengano crittografate durante il trasferimento e hashing con salt quando vengono memorizzate?
	Gestione degli accessi 3.2.3 - Gestione delle credenziali - Gestione segreta	Usi un servizio di gestione segreta?
	Gestione degli accessi 3.2.4 - Gestione delle credenziali - Credenziali nel codice (richiede l'attestazione manuale)	Le credenziali sono incluse nel codice sorgente?

Set di controlli	Titolo di controllo	Descrizione del controllo
Accesso all'ambiente di produzione	Gestione degli accessi 3.3.1 - Accesso all'ambiente di produzione - Single Sign-on (richiede un'attestazione manuale)	L'SSO è abilitato all'accesso all'ambiente di produzione?
	Gestione degli accessi 3.3.2 - Accesso all'ambiente di produzione - Autenticazione a due fattori	È necessaria l'autenticazione a due fattori per accedere all'ambiente di produzione?
	Gestione degli accessi 3.3.3 - Accesso all'ambiente di produzione - Utente root (richiede l'attestazione manuale)	L'utente root viene utilizzato solo in caso di emergenza per accedere all'ambiente di produzione?
	Gestione degli accessi 3.3.4 - Accesso all'ambiente di produzione - MFA utente root	L'utente root richiede l'autenticazione a due fattori (MFA)?
	Gestione degli accessi 3.3.5 - Accesso all'ambiente di produzione - Accesso remoto	L'accesso remoto all'ambiente di produzione è protetto mediante meccanismi quali VPN o autenticazione basata su chiavi?
Politica di controllo degli accessi	Gestione degli accessi 3.4.1 - Politica di controllo degli accessi - Accesso con privilegi minimi	Seguite la politica di accesso con privilegi minimi per consentire agli utenti di accedere all'ambiente di produzione?
	Gestione degli accessi 3.4.2 - Politica di controllo degli accessi - Revisione della politica di accesso	Tutte le politiche di accesso nell'ambiente di produzione vengono riviste regolarmente?

Set di controlli	Titolo di controllo	Descrizione del controllo
	Gestione degli accessi 3.4.3 - Politica di controllo degli accessi - Configurazione degli utenti e delle politiche di sicurezza (richiede l'attestazione manuale)	L'applicazione consente ai clienti di gestire i propri utenti e i relativi privilegi?
	Gestione degli accessi 3.4.4 - Politica di controllo degli accessi - Segmentazione logica (richiede l'attestazione manuale)	Esiste una segmentazione logica delle applicazioni?
	Gestione degli accessi 3.4.5 - Politica di controllo degli accessi - Revisione dell'accesso al momento della cessazione	Tutte le politiche di accesso pertinenti sono aggiornate in caso di licenziamento del dipendente?
Registri di accesso	Gestione degli accessi 3.5.1 - Registri di accesso	Vengono registrate le attività eseguite dagli utenti nell'ambiente di produzione?

Controlli di sicurezza delle applicazioni

I controlli di sicurezza delle applicazioni verificano se la sicurezza è stata incorporata nell'applicazione durante la progettazione, lo sviluppo e il test. Questa tabella elenca i valori e le descrizioni per i controlli delle policy di sicurezza delle applicazioni.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Ciclo di vita sicuro dello sviluppo del software	Application Security 4.1.1 - Ciclo di vita di sviluppo del software sicuro	L'ambiente di sviluppo, test e staging è separato	Specificate se l'ambiente di sviluppo, test e gestione temporane	Si

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	- Ambiente separato	dall'ambiente di produzione?	a è separato dall'ambiente di produzione.	
	Sicurezza delle applicazioni 4.1.2 - Ciclo di vita di sviluppo sicuro del software - Pratica di codifica sicura	I tecnici della sicurezza collaborano con gli sviluppatori sulle pratiche di sicurezza?	Specificate se gli sviluppatori e i tecnici della sicurezza collaborano su pratiche di codifica sicure.	Sì
	Sicurezza delle applicazioni 4.1.3 - Ciclo di vita sicuro dello sviluppo del software - Utilizzo dei dati dei clienti nell'ambiente di test (richiede l'attestazione manuale)	I dati dei clienti vengono mai utilizzati negli ambienti di test, sviluppo o controllo qualità?	I dati dei clienti vengono mai utilizzati negli ambienti di test, sviluppo o controllo qualità? In caso affermativo, quali dati vengono utilizzati e a cosa servono?	No

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Sicurezza delle applicazioni 4.1.4 - Ciclo di vita di sviluppo del software sicuro - Connessione sicura	SSL/TLS è abilitato per tutte le pagine Web e le comunicazioni che utilizzano i dati dei clienti?	Specificate se viene utilizzata una connessione sicura (come SSL/TLS) per tutte le comunicazioni con i dati dei clienti.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Sicurezza delle applicazioni 4.1.5 - Ciclo di vita sicuro dello sviluppo del software - Backup delle immagini	Viene eseguito il backup delle istantanee delle immagini delle applicazioni?	Specificate se viene eseguito il backup delle istantanee delle immagini (ad esempio i sistemi che supportano o l'applicazione e i sistemi che ospitano i dati dei clienti). In caso affermativo, esiste una procedura per garantire che le istantanee e di immagini contenenti dati relativi all'ambito o siano autorizzate prima di essere scattate? Il controllo degli accessi è implementato per le istantanee delle immagini?	Sì. Il backup delle immagini viene eseguito con l'approvazione del cliente e della direzione.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Revisione della sicurezza delle applicazioni	Sicurezza delle applicazioni 4.2.1 - Revisione della sicurezza delle applicazioni - Revisione del codice sicuro	La revisione sicura del codice viene effettuata a prima di ogni versione?	Specificate se viene effettuata a una revisione del codice di sicurezza prima di ogni versione.	Sì
	Sicurezza delle applicazioni 4.2.2 - Revisione della sicurezza delle applicazioni - Test di penetrazione	Vengono eseguiti test di penetrazione? Possiamo ricevere segnalazioni sui test di penetrazione?	Specificate se i test di penetrazione vengono eseguiti sull'applicazione. In caso affermativo, è possibile condividere gli ultimi 3 report come prove manuali?	Sì
	Application Security 4.2.3 - Revisione della sicurezza delle applicazioni - Patch di sicurezza	Tutte le patch di sicurezza ad alto rischio disponibili vengono applicate e verificate regolarmente?	Specificate se le patch di sicurezza ad alto rischio vengono applicate regolarmente. Se sì, con che frequenza vengono applicate?	Sì. Le patch di sicurezza vengono applicate mensilmente.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Application Security 4.2.4 - Revisione della sicurezza delle applicazioni - Scansioni di vulnerabilità sulle applicazioni	Le scansioni di vulnerabilità vengono eseguite su tutte le applicazioni con accesso a Internet regolarmente e dopo modifiche significative?	Specificate se le scansioni di vulnerabilità vengono eseguite su tutte le applicazioni con accesso a Internet. In caso affermativo, con quale frequenza vengono eseguite le scansioni di vulnerabilità? Possiamo avere una copia del rapporto?	Sì. Le scansioni di vulnerabilità vengono eseguite mensilmente.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Application Security 4.2.5 - Revisione della sicurezza delle applicazioni - Gestione delle minacce e delle vulnerabilità	Esistono processi per gestire gli strumenti di valutazione delle minacce e delle vulnerabilità e i dati che raccolgono?	Specificate se esistono processi per gestire gli strumenti di valutazione delle minacce e delle vulnerabilità e i relativi risultati. Potresti fornire maggiori dettagli su come vengono gestite le minacce e le vulnerabilità?	Sì. Tutte le minacce e le vulnerabilità provenienti da fonti diverse sono aggregate in un unico portale. Sono gestite in base alla gravità.
	Application Security 4.2.6 - Revisione della sicurezza delle applicazioni - Scansioni antimalware	La scansione antimalware viene eseguita regolarmente sulla rete e sui sistemi che ospitano l'applicazione?	Specificate se la scansione antimalware viene eseguita sulla rete e sui sistemi che ospitano l'applicazione. Se sì, con che frequenza viene eseguita? Puoi fornire il rapporto?	Sì. Le scansioni antimalware vengono eseguite mensilmente.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Registri delle applicazioni	Sicurezza delle applicazioni 4.3.1 - Registri delle applicazioni - Registri delle applicazioni	I registri delle applicazioni vengono raccolti e controllati?	Specificate se i registri delle applicazioni vengono raccolti e controllati. In caso affermativo, per quanto tempo vengono conservati i registri?	Sì. I registri vengono conservati per un anno.
	Application Security 4.3.2 - Registri delle applicazioni - Accesso ai registri	I registri del sistema operativo e delle applicazioni sono protetti da modifiche, eliminazioni e/o accessi inappropriati?	Specificate se i registri del sistema operativo e delle applicazioni sono protetti da modifiche, eliminazioni e/o accessi inappropriati. In caso di violazione o incidente, disponete di procedure per rilevare la perdita dei registri delle applicazioni?	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Application Security 4.3.3 - Registri delle applicazioni - Dati archiviati nei registri (richiede l'attestazione manuale)	Le informazioni di identificazione personale (PII) del cliente vengono archiviate nei registri?	Specificate se memorizzate le informazioni di identificazione personale (PII) del cliente nei registri.	No. Nessun dato PII verrà memorizzato nei registri.
Modifica la politica di controllo	Sicurezza delle applicazioni 4.4.1 - Politica di controllo delle modifiche - Test funzionali e di resilienza	I test funzionali e di resilienza vengono eseguiti prima di rilasciare e una modifica?	Specificate se i test funzionali e di resilienza vengono eseguiti sull'applicazione prima di una nuova versione.	Sì
	Sicurezza delle applicazioni 4.4.2 - Politica di controllo delle modifiche - Procedure di controllo delle modifiche	Le procedure di controllo delle modifiche sono necessarie per tutte le modifiche all'ambiente di produzione?	Specificate se le procedure di controllo delle modifiche sono valide per tutte le modifiche apportate nell'ambiente di produzione.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	Application Security 4.4.3 - Change Control Policy - Evita errori e rischi umani nella produzione	Disponete di un processo per verificare che l'errore umano e i rischi non vengano messi in produzione?	Specificate che esiste un processo per verificare che l'errore umano e i rischi non vengano trasferiti alla produzione.	Sì
	Application Security 4.4.4 - Politica di controllo delle modifiche - Modifiche ai documenti e ai registri	Documentate e registrate le modifiche che possono influire sui servizi?	Specificate se le modifiche che influiscono sui servizi sono documentate e registrate. In caso affermativo, per quanto tempo vengono conservati i registri?	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	Application Security 4.4.5 - Politica di controllo delle modifiche - Notifica di modifica per gli acquirenti (richiede un'attestazione manuale)	Esiste una procedura formale per garantire che i clienti vengano informati prima che vengano apportate modifiche che potrebbero influire sul servizio offerto?	Specificate se i clienti riceveranno una notifica prima di apportare modifiche che potrebbero influire sul loro servizio. In caso affermativo, qual è lo SLA per notificare ai clienti le modifiche che influiscono?	Sì. Informiamo i clienti 90 giorni prima che influiscano sulle modifiche.

Controlli di audit e conformità

I controlli di audit e conformità valutano l'adesione di un'organizzazione ai requisiti normativi. Questa tabella elenca i valori e le descrizioni per i controlli di audit e conformità.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
Certificazioni complete	Audit e conformità 1.1.1 - Certificazioni complete (richiede l'attestazione manuale)	Elenca le certificazioni che possiedi.	Specificate quali certificazioni possedete.	SOC2, ISO/IEC 27001
Certificazione in corso	Audit e conformità 1.2.1 - Certificazione	Elenca i certificati aggiuntivi	Elenca tutti i certificati	Sì. La certificazione PCI è in

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	zione in corso (richiede l'attestazione manuale)	attualmente in corso.	aggiuntivi attualmente in fase di verifica o revisione con una data di completamento stimata.	corso (ETA Q2 2022).
Procedure che garantiscono la conformità	Audit e conformità a 1.3.1 - Procedure che garantiscono la conformità - Procedure che garantiscono la conformità	Disponete di una politica o di una procedura per garantire la conformità ai requisiti legislativi, regolamentari e contrattuali applicabili?	Specificate se avete una politica o una procedura per garantire la conformità ai requisiti legislativi, regolamentari e contrattuali applicabili. In caso affermativo, elenca i dettagli sulla procedura e carica le prove manuali.	Sì. Abbiamo caricato documenti come SOC2, ISO/IEC 27001.
	Audit e conformità a 1.3.2 - Procedure che garantiscono la conformità - Audit per tenere traccia dei requisiti in sospeso	Gli audit sono stati completati per tracciare i requisiti normativi e di conformità in sospeso?	Specificate se vengono effettuati audit per tenere traccia dei requisiti in sospeso. In caso affermativo, fornisci i dettagli.	Sì, gli audit vengono effettuati mensilmente per tenere traccia dei requisiti in sospeso.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Audit e conformità 1.3.3 - Procedure che garantiscono la conformità - Deviazioni ed eccezioni (richiede l'attestazione manuale)	Disponete di un processo per gestire le deviazioni e le eccezioni dai requisiti di conformità?	Specificate se esiste un processo per gestire le eccezioni o le deviazioni dai requisiti di conformità. In caso affermativo, fornisci i dettagli.	Sì. Disponiamo di un registro delle deviazioni e di strumenti di segnalazione. Esaminiamo ogni eccezione o deviazione per prevenire che si verifichino future.

Controlli di resilienza aziendale

I controlli di resilienza aziendale valutano la capacità dell'organizzazione di adattarsi rapidamente alle interruzioni mantenendo al contempo la continuità aziendale. Questa tabella elenca i valori e le descrizioni per i controlli delle politiche di resilienza aziendale.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
Resilienza aziendale	Resilienza e continuità aziendale 6.1.1 - Resilienza aziendale - Test di failover (richiede un'attestazione manuale)	I test di failover del sito vengono eseguiti almeno una volta all'anno?	Specificate se i test di failover vengono eseguiti ogni anno. In caso negativo, con che frequenza vengono eseguiti?	Sì
	Resilienza e continuità	È stata condotta un'analisi	Specificare se è stata eseguita	Sì. Un'analisi dell'impatto

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	aziendale 6.1.2 - Resilienza aziendale - Analisi dell'impatto aziendale (richiede l'attestazione manuale)	dell'impatto aziendale?	un'analisi dell'impatto aziendale. In caso affermativo, quando è stata completata l'ultima volta? Fornire dettagli sull'analisi condotta.	aziendale è stata completata 6 mesi fa.
	Resilienza e continuità aziendale 6.1.3 - Resilienza aziendale - Dipendenze da fornitori terzi (richiede l'attestazione manuale)	Esistono dipendenze da fornitori di servizi terzi essenziali (oltre a un fornitore di servizi cloud)?	Specificate se esiste una dipendenza da fornitori di terze parti (oltre a un fornitore di servizi cloud). Se sì, puoi fornire dettagli sui fornitori?	No
	Resilienza e continuità aziendale 6.1.4 - Resilienza aziendale - Test di continuità e ripristino di terze parti (richiede l'attestazione manuale)	È necessario che i fornitori di terze parti adottino i propri processi ed esercizi di disaster recovery?	Specificate se i fornitori di terze parti devono avere i propri processi ed esercizi di disaster recovery.	Non applicabile in questo esempio.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Resilienza e continuità aziendale 6.1.5 - Resilienza aziendale - Violazione del contratto da parte di fornitori terzi (richiede un'attestazione manuale)	I contratti con fornitori di servizi essenziali includono una clausola penale o riparativa in caso di violazione e della disponibilità e della continuità Sold and Shipped by Amazon (SSA)?	Le clausole penali o correttive e per la violazione e della disponibilità e della continuità sono incluse nei contratti con fornitori terzi?	Non applicabile in questo esempio.
	Resilienza e continuità aziendale 6.1.6 - Resilienza aziendale - Health of the System	Disponete di monitor o avvisi per comprendere lo stato del sistema?	Specificate se sono presenti monitor o avvisi per comprendere lo stato del sistema.	Sì
Continuità aziendale	Resilienza e continuità aziendale 6.2.1 - Continuità operativa - Politiche/procedure di continuità operativa	Le procedure formali di continuità aziendale sono sviluppate e documentate?	Specificate se le procedure formali sono sviluppate e mantenute per la continuità aziendale. In caso affermativo, fornire maggiori dettagli sulle procedure.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	Resilienza e continuità aziendale 6.2.2 - Continuità operativa - Strategie di risposta e ripristino	Sono state definite strategie di risposta e ripristino specifiche per le attività prioritarie?	Specificate se sono state sviluppate strategie di ripristino e risposta per le attività e i servizi dei clienti.	Sì
	Resilienza e continuità aziendale 6.2.3 - Continuità aziendale - Test di continuità operativa	Eseguite test di ripristino per garantire la continuità aziendale?	Specificate se eseguite test di ripristino per garantire la continuità aziendale in caso di guasto.	Sì. In caso di guasto, i sistemi per la continuità operativa verranno attivati entro 2 ore.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Resilienza e continuità aziendale 6.2.4 - Continuità operativa - Impatto sulla disponibilità in ambienti multi-tenancy (richiede l'attestazione manuale)	Limitate la capacità dell'acquirente di imporre un carico che potrebbe influire sulla disponibilità per gli altri utenti del sistema?	Specificate se il carico di un acquirent e può influire sulla disponibilità per un altro acquirente. In caso affermativo, qual è la soglia fino alla quale non vi sarà alcun impatto? In caso negativo, potete fornire maggiori dettagli su come garantire che i servizi non subiscano ripercussioni durante i picchi di utilizzo e oltre?	Sì. Soglia non disponibile per questo esempio.
Disponibilità dell'applicazione	Resilienza e continuità aziendale 6.3.1 - Disponibilità delle applicazioni - Record di disponibilità (richiede l'attestazione manuale)	Ci sono stati problemi significativi legati all'affidabilità o alla disponibilità nell'ultimo anno?	Specificare se si sono verificati i problemi significativi relativi all'affidabilità o alla disponibilità nell'ultimo anno.	No

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	<p>Resilienza e continuità aziendale 6.3.2</p> <p>- Disponibilità delle applicazioni - Finestra di manutenzione programmata (richiede l'attestazione manuale)</p>	<p>Sono previsti tempi di inattività durante la manutenzione programmata?</p>	<p>Specificate se è prevista una finestra di manutenzione programmata durante la quale i servizi potrebbero essere inattivi. Se sì, quanto dura il periodo di inattività?</p>	<p>No</p>
	<p>Resilienza e continuità aziendale 6.3.3</p> <p>- Disponibilità delle applicazioni</p> <p>- Portale online per gli incidenti (richiede l'attestazione manuale)</p>	<p>Esiste un portale online sullo stato della risposta agli incidenti che descrive le interruzioni pianificate e non pianificate?</p>	<p>Specificate se esiste un portale sullo stato degli incidenti che descriva le interruzioni pianificate e non pianificate. In caso affermativo, fornisci dettagli su come un cliente può accedervi. Quanto tempo dopo l'interruzione verrà aggiornato il portale?</p>	<p>Sì. Il cliente può accedere ai dettagli tramite example.com.</p>

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Resilienza e continuità aziendale 6.3.4 - Disponibilità delle applicazioni - Obiettivo del tempo di ripristino (richiede un'attestazione manuale)	Esiste un obiettivo RTO (Recovery Time Objective) specifico?	Specificare se esiste un Recovery Time Objective (RTO). In caso affermativo, è possibile fornire l'RTO?	Sì, un RTO di 2 ore.
	Resilienza e continuità aziendale 6.3.5 - Disponibilità delle applicazioni - Obiettivo Recovery Point (richiede un'attestazione manuale)	Esiste un Recovery Point Objective (RPO) specifico?	Specificare se esiste un Recovery Point Objective (RPO). In caso affermativo, è possibile fornire l'RPO?	Sì, un RPO di 1 settimana.

Controlli di sicurezza dei dati

I controlli di sicurezza dei dati proteggono dati e risorse. Questa tabella elenca i valori e le descrizioni per i controlli di sicurezza dei dati.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Dati dei clienti acquisiti	Data Security 2.1.1 - Dati dei	Crea un elenco di dati necessari	Descrivi tutti i dati utilizzati	Non viene utilizzato alcun

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	clienti inseriti (richiede l'attestazione manuale)	ai clienti per la funzionalità del prodotto.	i dai clienti. Specificate se vengono utilizzati i dati sensibili o riservati.	dato sensibile e riservato. Questo prodotto utilizza solo informazioni non sensibili come i log delle applicazioni, dell'infrastruttura e. Servizi AWS (AWS CloudTrail, AWS Config, Log di flusso in VPC)
Posizione di archiviazione dei dati	Sicurezza dei dati 2.2.1 - Posizione di archiviazione dei dati (richiede l'attestazione manuale)	Dove vengono archiviati i dati dei clienti? Elenca i paesi e le regioni in cui sono archiviati i dati.	Specificare l'elenco dei paesi e delle regioni in cui vengono archiviati i dati.	Ohio (Stati Uniti), Oregon (Stati Uniti), Irlanda (UE)

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Controllo degli accessi	Data Security 2.3.1 - Controllo degli accessi - Accesso dei dipendenti (richiede l'attestazione manuale)	I dipendenti hanno accesso ai dati non crittografati dei clienti?	Specificate se i dipendenti hanno accesso ai dati non crittografati dei clienti. In caso affermativo, spiega brevemente perché hanno bisogno dell'accesso. In caso negativo, spiegate brevemente come controllate l'accesso.	No, tutti i dati vengono crittografati quando vengono archiviati. I dipendenti non avranno accesso ai dati dei clienti ma solo ai dati relativi al loro utilizzo.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Data Security 2.3.2 - Controllo degli accessi - Applicazione mobile (richiede l'attestazione manuale)	I clienti possono accedere ai propri dati tramite un'applicazione mobile?	Specificate se i clienti possono accedere ai propri dati utilizzando un'applicazione mobile. In caso affermativo, fornisci maggiori dettagli. Come fanno i clienti ad accedere? Le credenziali vengono memorizzate nella cache dell'applicazione? Con che frequenza vengono aggiornati i token?	No, non è possibile accedere al servizio utilizzando un'applicazione mobile.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Sicurezza dei dati 2.3.3 - Controllo degli accessi - Paesi a cui vengono trasmessi i dati (richiede un'attestazione manuale)	I dati dei clienti vengono trasmessi a paesi diversi da quelli di origine?	I dati dei clienti vengono trasmessi in paesi al di fuori dell'origine? In caso affermativo, specifica l'elenco dei paesi in cui i dati dei clienti vengono trasmessi o ricevuti.	No
	Sicurezza dei dati 2.3.4 - Controllo degli accessi - I dati vengono condivisi con fornitori terzi (richiede l'attestazione manuale)	I dati dei clienti vengono condivisi con fornitori di terze parti (diversi dai fornitori di servizi cloud)?	I dati dei clienti vengono condivisi con fornitori terzi? In caso affermativo, specifica l'elenco dei fornitori di terze parti e i relativi paesi o regioni in cui fornisci i dati dei clienti.	No

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Sicurezza dei dati 2.3.5 - Controllo degli accessi - Politica di sicurezza relativa ai fornitori di terze parti	Disponete di politiche o procedure per garantire che i fornitori terzi mantengano la riservatezza, la disponibilità e l'integrità dei dati dei clienti?	Specificate se disponete di politiche o procedure per garantire che i fornitori terzi mantengano la riservatezza, la disponibilità e l'integrità dei dati dei clienti. In caso affermativo, carica un manuale o un documento delle politiche o delle procedure.	Non applicabile in questo esempio.
Crittografia dei dati	Sicurezza dei dati 2.4.1 - Crittografia dei dati - Crittografia dei dati a riposo	Tutti i dati sono criptati quando sono inattivi?	Specificate se tutti i dati sono criptati quando sono inattivi.	Sì
	Data Security 2.4.2 - Crittografia dei dati - Crittografia dei dati in transito	Tutti i dati sono crittografati in transito?	Specificate se tutti i dati sono crittografati in transito.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Data Security 2.4.3 - Crittografia dei dati - Algoritmi avanzati (richiede l'attestazione manuale)	Utilizzate algoritmi di crittografia avanzati?	Utilizzate algoritmi di crittografia avanzati? In caso affermativo, specifica quali algoritmi di crittografia (come RSA, AES 256) vengono utilizzati.	Sì. AES 256 viene utilizzato per crittografare i dati.
	Data Security 2.4.4 - Crittografia dei dati - Chiave di crittografia unica (richiede l'attestazione manuale)	I clienti hanno la possibilità di generare una chiave di crittografia unica?	I clienti possono fornire o generare le proprie chiavi di crittografia uniche? In caso affermativo, fornisci maggiori dettagli e carica le prove.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Data Security 2.4.5 - Crittografia dei dati - Accesso alle chiavi di crittografia (richiede l'attestazione manuale)	Ai dipendenti viene impedito l'accesso alle chiavi di crittografia di un cliente?	Specificate se ai vostri dipendenti viene impedito l'accesso alle chiavi di crittografia di un cliente. In caso negativo, spiega perché hanno accesso alle chiavi del cliente. In caso affermativo, spiega come viene controllato l'accesso.	Sì. Le chiavi crittografiche vengono archiviate in modo sicuro e ruotate periodicamente. I dipendenti non hanno accesso a queste chiavi.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Archiviazione e classificazione dei dati	Sicurezza dei dati 2.5.1 - Archiviazione e classificazione dei dati - Backup dei dati	Eseguite il backup dei dati dei clienti?	Specificare se si esegue il backup dei dati dei clienti. In caso affermativo, descrivi la tua politica di backup (compresi i dettagli sulla frequenza con cui viene eseguito il backup, dove viene archiviato il backup, sulla crittografia e sulla ridondanza dei backup).	Sì, il backup viene eseguito ogni tre mesi. Il backup è crittografato e archiviato nella stessa area dei dati del cliente. Il tecnico dell'assistenza del cliente ha accesso al ripristino del backup ma non ai dati in esso contenuti.
	Sicurezza dei dati 2.5.2 - Archiviazione e classificazione dei dati - Politica di controllo dell'accesso ai dati	Implementate controlli di accesso appropriati per i dati archiviati dei clienti? Fornisci le tue politiche di controllo degli accessi.	Specificate se sono implementati controlli di accesso appropriati (come RBAC) per i dati archiviati dei clienti. Fornisci maggiori dettagli e prove manuali su come controlli l'accesso ai dati.	Sì. I controlli di accesso con privilegi minimi vengono implementati per limitare l'accesso ai dati dei clienti.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Sicurezza dei dati 2.5.3 - Archiviazione e classificazione dei dati - Dati delle transazioni (richiede l'attestazione manuale)	I dettagli delle transazioni del cliente (come i dati della carta di pagamento e le informazioni sui gruppi che effettuano le transazioni) sono archiviati in una zona perimetrale?	Specificate se i dettagli delle transazioni del cliente (come i dati della carta di pagamento e le informazioni sui gruppi che effettuano le transazioni) verranno archiviati in una zona perimetrale. In caso affermativo, spiega perché deve essere archiviato nella zona perimetrale.	No
	Sicurezza dei dati 2.5.4 - Archiviazione e classificazione dei dati - Classificazione delle informazioni	I dati dei clienti sono classificati in base ai requisiti legali o normativi, al valore aziendale e alla sensibilità alla divulgazione o alla modifica non autorizzata?	Specificate se i dati dei clienti sono classificati in base alla sensibilità. In caso affermativo, carica le prove manuali di questa classificazione.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Data Security 2.5.5 - Archiviazione e classificazione dei dati - Segmentazione dei dati (richiede un'attestazione manuale)	Viene fornita la funzionalità di segmentazione e separazione dei dati tra i clienti?	Specificate se i dati per diversi clienti sono segmentati. In caso negativo, spiegate i meccanismi a vostra disposizione per proteggere i dati dalla contaminazione incrociata.	Sì
Conservazione dei dati	Data Security 2.6.1 - Conservazione dei dati (richiede l'attestazione manuale)	Per quanto tempo conservate i dati?	Specificare la durata della conservazione dei dati. Se il periodo di conservazione differisce in base alla classificazione e alla sensibilità dei dati, è possibile fornire dettagli su ciascun periodo di conservazione?	6 mesi

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Conservazione dei dati dopo l'annullamento dell'iscrizione degli acquirenti	Sicurezza dei dati 2.6.2 - Conservazione dei dati dopo l'annullamento dell'iscrizione del cliente (richiede un'attestazione manuale)	Per quanto tempo conservate e i dati dopo l'annullamento dell'iscrizione degli acquirenti?	Specificate la durata della conservazione dei dati dopo l'annullamento dell'iscrizione dei clienti.	3 mesi

Controlli di sicurezza dei dispositivi degli utenti finali

I controlli di sicurezza dei dispositivi degli utenti finali proteggono i dispositivi portatili degli utenti finali e le reti a cui sono collegati da minacce e vulnerabilità. Questa tabella elenca i valori e le descrizioni per i controlli delle policy di sicurezza dei dispositivi degli utenti finali.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Inventario di asset/software	End User Device Security 7.1.1 - Inventario di asset/software - Inventario degli asset	L'elenco dell'inventario delle risorse viene aggiornato periodicamente?	Specificate se viene mantenuto un inventario degli asset. Se sì, con che frequenza viene aggiornato?	Sì. L'inventario viene aggiornato settimanalmente.
	End User Device Security 7.1.2 - Inventario di risorse/software - Inventario	Tutte le piattaforme e le applicazioni software installate sui sistemi con	Specificate se viene mantenuto l'inventario di tutti i software e le applicazioni	Sì. L'inventario viene aggiornato settimanalmente.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	di software e applicazioni	ambito sono inventariate?	oni installati. Se sì, con che frequenza viene aggiornato?	
Sicurezza delle risorse	Sicurezza dei dispositivi degli utenti finali 7.2.1 - Sicurezza degli asset - Patch di sicurezza	Tutte le patch di sicurezza ad alto rischio disponibili vengono applicate e verificate almeno una volta al mese su tutti i dispositivi degli utenti finali?	Specificate se tutte le patch di sicurezza ad alto rischio vengono applicate almeno una volta al mese. In caso negativo, con che frequenza viene applicato? Potete fornire maggiori dettagli su come gestite le patch?	Sì. Abbiamo un team di sicurezza che esegue questo processo ogni due settimane.
	Sicurezza dei dispositivi degli utenti finali 7.2.2 - Asset Security - Endpoint Security	Disponete della sicurezza degli endpoint?	Specificate se la sicurezza degli endpoint è installata su tutti i dispositivi. In caso affermativo, potete fornire maggiori dettagli sullo strumento e su come viene gestito?	Sì. Il nostro team di sicurezza lo gestisce ogni due settimane utilizzando strumenti interni.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	End User Device Security 7.2.3 - Sicurezza degli asset - Manutenzione e riparazione degli asset (richiede un'attestazione manuale)	La manutenzione e la riparazione delle risorse organizzative vengono eseguite e registrate con strumenti approvati e controllati?	Specificate se la manutenzione e la riparazione delle risorse vengono eseguite e registrate con strumenti controllati. In caso affermativo, potreste fornire maggiori dettagli su come viene gestita?	Sì. Tutte le operazioni di manutenzione dei dispositivi vengono registrate e. Questa manutenzione non comporta tempi di inattività.
	End User Device Security 7.2.4 - Asset Security - Controllo degli accessi per i dispositivi	I dispositivi hanno il controllo degli accessi abilitato?	Specificate se i dispositivi hanno i controlli di accesso (come RBAC) abilitati.	Sì. L'accesso con privilegi minimi è implementato per tutti i dispositivi.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Registri dei dispositivi	End User Device Security 7.3.1 - Registri dei dispositivi - Dettagli sufficienti nei registri (richiede un'attestazione manuale)	I dati registrati nei registri del sistema operativo e del dispositivo sono sufficienti a supportare le indagini sugli incidenti?	Specificate se nei registri sono inclusi dettagli sufficienti (come i tentativi di accesso riusciti e falliti e le modifiche a impostazioni e file di configurazione sensibili) per supportare le indagini sugli incidenti. In caso negativo, fornisci maggiori dettagli su come gestisci le indagini sugli incidenti.	Sì
	End User Device Security 7.3.2 - Registri dei dispositivi - Accesso ai registri dei dispositivi	I registri dei dispositivi sono protetti da modifiche , eliminazioni e/o accessi inappropriati?	Specificate se i registri del dispositivo sono protetti da modifiche , cancellazioni e/o accessi inappropriati. In caso affermativo, puoi fornire dettagli su come applicarlo?	Sì. Le modifiche ai registri vengono applicate tramite il controllo degli accessi. Tutte le modifiche ai registri generano un avviso.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	End User Device Security 7.3.3 - Registri dei dispositivi - Conservazione dei log (richiede un'attestazione manuale)	I log vengono conservati per un periodo di tempo sufficiente a indagare su un attacco?	Per quanto tempo verranno conservati i log?	Sì, 1 anno.
Gestione dei dispositivi mobili	End User Device Security 7.4.1 - Gestione dei dispositivi mobili - Programma di gestione dei dispositivi mobili	Esiste un programma di gestione dei dispositivi mobili?	Specificare se esiste un programma di gestione dei dispositivi mobili. In caso affermativo, specifica quale strumento viene utilizzato per la gestione dei dispositivi mobili.	Sì. Utilizziamo strumenti interni.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	End User Device Security 7.4.2 - Gestione dei dispositivi mobili - Accesso all'ambiente di produzione da dispositivi mobili privati (richiede l'attestazione manuale)	Al personale viene impedito l'accesso all'ambiente di produzione e utilizzando dispositivi mobili privati non gestiti?	Specificate se ai dipendenti viene impedito l'accesso all'ambiente di produzione e utilizzando dispositivi mobili privati non gestiti. Se no, come si fa a far rispettare questo controllo?	Sì
	End User Device Security 7.4.3 - Gestione dei dispositivi mobili - Accesso ai dati dei clienti dai dispositivi mobili (richiede un'attestazione manuale)	Ai dipendenti viene impedito di utilizzare dispositivi mobili privati non gestiti per visualizzare o elaborare i dati dei clienti?	Specificate se ai dipendenti viene impedito l'accesso ai dati dei clienti utilizzando dispositivi mobili non gestiti. In caso negativo, qual è il caso d'uso per consentire l'accesso? Come si monitora l'accesso?	Sì

Controlli delle risorse umane

I controlli delle risorse umane valutano la divisione relativa ai dipendenti per la gestione dei dati sensibili durante processi quali l'assunzione, il pagamento e il licenziamento dei dipendenti. Questa tabella elenca i valori e le descrizioni per i controlli delle politiche relative alle risorse umane.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Politica delle risorse umane	Risorse umane 9.1.1 - Politica delle risorse umane - Analisi dei precedenti per i dipendenti	Lo screening dei precedenti viene effettuato prima dell'assunzione?	Specificate se lo screening dei precedenti viene effettuato per tutti i dipendenti prima dell'assunzione.	Sì
	Risorse umane 9.1.2 - Politica delle risorse umane - Contratto per i dipendenti	Un contratto di lavoro viene firmato prima dell'assunzione?	Specificare se un contratto di lavoro viene firmato prima dell'assunzione.	Sì
	Risorse umane 9.1.3 - Politica delle risorse umane - Formazione sulla sicurezza per i dipendenti	Tutti i dipendenti si sottopongono regolarmente a corsi di sensibilizzazione alla sicurezza?	Specificate se i dipendenti seguono regolarmente corsi di formazione sulla sicurezza. Se sì, con che frequenza si sottopongono a corsi di	Sì. Si sottopongono a corsi di formazione sulla sicurezza ogni anno.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
			formazione sulla sicurezza?	
	Risorse umane 9.1.4 - Politica delle risorse umane - Processo disciplinare per la non conformità delle politiche	Esiste un processo disciplinare per la non conformità delle politiche in materia di risorse umane?	Specificare se esiste un processo disciplinare per la non conformità delle politiche in materia di risorse umane.	Sì
	Risorse umane 9.1.5 - Politica delle risorse umane - Controlli dei precedenti per appaltatori/subappaltatori (richiede l'attestazione manuale)	I controlli dei precedenti vengono eseguiti per fornitori, appaltatori e subappaltatori di terze parti?	Specificate se vengono effettuati controlli sui precedenti per fornitori, appaltatori e subappaltatori di terze parti. In caso affermativo, il controllo dei precedenti viene eseguito regolarmente?	Sì. Il controllo dei precedenti viene effettuato ogni anno.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Risorse umane 9.1.6 - Politica delle risorse umane - Restituzione dei beni in caso di risoluzione	Esiste una procedura per verificare la restituzione dei beni costitutivi al momento della cessazione?	Specificare se esiste una procedura per verificare la restituzione dei beni costituiti in caso di licenziamento del dipendente.	Si

Controlli di sicurezza dell'infrastruttura

I controlli di sicurezza dell'infrastruttura proteggono le risorse critiche da minacce e vulnerabilità. Questa tabella elenca i valori e le descrizioni per i controlli delle politiche di sicurezza dell'infrastruttura.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Sicurezza fisica	Sicurezza dell'infrastruttura 8.1.1 - Sicurezza fisica - Accesso fisico alle strutture	Le persone che richiedono o l'accesso di persona alle risorse (come edifici, veicoli o hardware) sono tenute a fornire un documento d'identità e tutte le credenziali necessarie?	Specificate se le persone che richiedono o l'accesso alle risorse di persona (come edifici, veicoli, hardware) sono tenute a fornire un ID e le eventuali	Si

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
			credenziali necessarie.	
	Sicurezza dell'infrastruttura 8.1.2 - Sicurezza fisica - Sicurezza fisica e controlli ambientali in atto	La sicurezza fisica e i controlli ambientali sono in atto nei data center e negli edifici adibiti a uffici?	Specificate se sono previsti controlli di sicurezza fisica e ambientale per tutte le strutture.	Sì
	Sicurezza dell'infrastruttura 8.1.3 - Sicurezza fisica - Accesso dei visitatori (richiede l'attestazione manuale)	Registrate l'accesso dei visitatori?	Se i visitatori sono ammessi nella struttura, vengono conservati i registri di accesso dei visitatori? Se sì, per quanto tempo vengono conservati i registri?	Sì. I registri verranno conservati per un anno.
Sicurezza della rete	Sicurezza dell'infrastruttura 8.2.1 - Sicurezza della rete: disabilita porte e servizi non utilizzati (richiede l'attestazione manuale)	Tutte le porte e i servizi non utilizzati sono disabilitati dall'ambiente e dai sistemi di produzione?	Specificare se tutte le porte e i servizi non utilizzati sono disabilitati dall'ambiente e dai sistemi di produzione.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Sicurezza dell'infrastruttura 8.2.2 - Sicurezza della rete - Uso dei firewall	I firewall vengono utilizzati per isolare i sistemi critici e sensibili in segmenti di rete separati dai segmenti di rete con sistemi meno sensibili?	Specificate se i firewall vengono utilizzati per isolare i segmenti critici e sensibili dai segmenti con sistemi meno sensibili.	Sì
	Sicurezza dell'infrastruttura 8.2.3 - Sicurezza della rete - Revisione delle regole del firewall	Tutte le regole relative ai firewall vengono riviste e aggiornate regolarmente?	Con che frequenza vengono riviste e aggiornate le regole del firewall?	Sì. Le regole del firewall vengono aggiornate ogni 3 mesi.
	Sicurezza dell'infrastruttura 8.2.4 - Sicurezza della rete - Sistemi di rilevamento/prevenzione delle intrusioni	I sistemi di rilevamento e prevenzione delle intrusioni sono implementati in tutte le zone di rete sensibili e ovunque siano abilitati i firewall?	Specificate se i sistemi di rilevamento e prevenzione delle intrusioni sono abilitati in tutte le zone di rete sensibili.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Sicurezza dell'infrastruttura 8.2.5 - Sicurezza della rete - Standard di sicurezza e rafforzamento	Disponete di standard di sicurezza e rafforzamento per i dispositivi di rete?	Specificate se disponete di standard di sicurezza e rafforzamento per i dispositivi di rete. In caso affermativo, potete fornire maggiori dettagli (compresi i dettagli sulla frequenza con cui questi standard vengono implementati e aggiornati)?	Sì. Gli standard di sicurezza e rafforzamento vengono implementati mensilmente sui dispositivi di rete.
Servizi cloud	Sicurezza dell'infrastruttura a 8.3.1 - Servizi cloud - Piattaforme utilizzate per ospitare l'applicazione (richiede l'attestazione manuale)	Elenca le piattaforme cloud che utilizzi per ospitare la tua applicazione.	Specificate quali piattaforme cloud utilizzate per ospitare la vostra applicazione.	AWS

Gestione del rischio e controlli della risposta agli incidenti

I controlli sulla gestione del rischio e sulla risposta agli incidenti valutano il livello di rischio ritenuto accettabile e le misure adottate per rispondere a rischi e attacchi. Questa tabella elenca i valori e le descrizioni per i controlli delle politiche di gestione del rischio e di risposta agli incidenti.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Valutazione del rischio	Gestione del rischio/risposta agli incidenti 5.1.1 - Valutazione del rischio: affrontare e identificare i rischi	Esiste un processo formale incentrato sull'identificazione e la risoluzione dei rischi di incidenti dirompenti per l'organizzazione?	Specificate se esiste un processo per identificare e affrontare i rischi che causano incidenti dirompenti per l'organizzazione.	Si
	Gestione del rischio/risposta agli incidenti 5.1.2 - Valutazione del rischio - Processo di gestione del rischio	Esiste un programma o un processo per gestire il trattamento dei rischi identificati durante le valutazioni?	Specificate se esiste un programma o un processo per gestire i rischi e le relative mitigazioni. In caso affermativo, potete fornire maggiori dettagli sul processo di gestione del rischio?	<p>Si. Esaminiamo e risolviamo o regolarmente i problemi per risolvere le non conformità. Le seguenti informazioni vengono identificate per qualsiasi problema che influisca sul nostro ambiente:</p> <ul style="list-style-type: none"> • Dettagli del problema identificato

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
				<ul style="list-style-type: none"> • Causa principale • Controlli di compensazione • Severità • Proprietario • Percorso da seguire a breve termine • Percorso a lungo termine
	<p>Gestione del rischio/risposta agli incidenti</p> <p>5.1.3 - Valutazione del rischio - Valutazioni del rischio</p>	<p>Le valutazioni del rischio vengono eseguite frequentemente?</p>	<p>Le valutazioni del rischio vengono effettuate frequentemente?</p> <p>In caso affermativo, specificare la frequenza delle valutazioni del rischio.</p>	<p>Sì. Le valutazioni del rischio vengono completate ogni 6 mesi.</p>

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Gestione del rischio/risposta agli incidenti 5.1.4 - Valutazione del rischio - Valutazione del rischio dei fornitori terzi	Le valutazioni del rischio vengono eseguite per tutti i fornitori di terze parti?	Specificate se le valutazioni del rischio vengono eseguite per tutti i fornitori di terze parti. In caso affermativo, con quale frequenza?	Non applicabile in questo esempio.
	Gestione del rischio/risposta agli incidenti 5.1.5 - Valutazione del rischio - Rivalutazione del rischio in caso di modifiche contrattuali	Le valutazioni del rischio vengono eseguite quando si verificano o la fornitura del servizio o le modifiche contrattuali?	Specificate se le valutazioni del rischio verranno eseguite ogni volta che una fornitura di servizi o un contratto cambia.	Non applicabile in questo esempio.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Gestione del rischio/risposta agli incidenti 5.1.6 - Valutazione del rischio - Accettazione dei rischi (richiede un'attestazione manuale)	Esiste un processo che consente alla direzione di accettare i rischi in modo consapevole e obiettivo e approvare i piani d'azione?	Specificate se esiste un processo che consente alla direzione di comprendere e accettare i rischi e di approvare i piani d'azione e una tempistica per risolvere un problema relativo al rischio. Il processo include la fornitura di dettagli sulle metriche alla base di ogni rischio alla direzione?	Sì. I dettagli sulla gravità del rischio e sui potenziali problemi, se non mitigati, vengono forniti alla direzione prima dell'approvazione del rischio.
	Gestione del rischio/risposta agli incidenti 5.1.7 - Valutazione del rischio - Metriche del rischio (richiede l'attestazione manuale)	Disponete di misure per definire, monitorare e segnalare le metriche di rischio?	Specificate se esiste un processo per definire, monitorare e segnalare le metriche di rischio.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Gestione degli incidenti	Gestione del rischio/Risposta agli incidenti 5.2.1 - Gestione degli incidenti - Piano di risposta agli incidenti	Esiste un piano di risposta agli incidenti formale?	Specificare se esiste un piano di risposta agli incidenti formale.	Sì
	Gestione del rischio/risposta agli incidenti 5.2.2 - Gestione degli incidenti - Contatto per segnalare incidenti di sicurezza (richiede l'attestazione manuale)	Esiste una procedura che consente ai clienti di segnalare un incidente di sicurezza?	Specificate se esiste una procedura che consente ai clienti di segnalare un incidente di sicurezza. In caso affermativo, come può un cliente segnalare un incidente di sicurezza?	Sì. I clienti possono segnalare gli incidenti a example.com.
	Gestione del rischio/risposta agli incidenti 5.2.3 - Gestione degli incidenti - Segnala incidenti /attività chiave	Segnate le attività chiave?	Segnate le attività chiave? Qual è lo SLA per la segnalazione delle attività chiave?	Sì. Tutte le attività chiave verranno segnalate entro una settimana.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Gestione del rischio/Risposta agli incidenti 5.2.4 - Gestione degli incidenti - Ripristino degli incidenti	Disponete di piani di disaster recovery?	Specificate se avete piani per il ripristino dopo che si è verificato un incidente. In caso affermativo, è possibile condividere i dettagli sui piani di ripristino?	Sì. Dopo un incidente, il ripristino verrà effettuato entro 24 ore.
	Gestione del rischio/risposta agli incidenti 5.2.5 - Gestione degli incidenti - Registri disponibili per gli acquirenti in caso di attacco (richiede un'attestazione manuale)	In caso di attacco, le risorse pertinenti (come registri, rapporti sugli incidenti o dati) saranno disponibili per i clienti?	Le risorse pertinenti (come registri, rapporti sugli incidenti o dati) relative al loro utilizzo saranno disponibili ai clienti in caso di attacco o incidente?	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'azione delle prove	Valore del campione
	Gestione del rischio/risposta agli incidenti 5.2.6 - Gestione degli incidenti - Bollettino sulla sicurezza (richiede l'attestazione manuale)	Disponete di un bollettino sulla sicurezza che descrive gli attacchi e le vulnerabilità più recenti che interessano le vostre applicazioni?	Specificate se disponete di un bollettino sulla sicurezza che descrive gli attacchi e le vulnerabilità più recenti che interessano le vostre applicazioni. In caso affermativo, potete fornire i dettagli?	Sì. I clienti possono segnalare gli incidenti a example.com.
Rilevamento degli incidenti	Gestione del rischio/risposta agli incidenti 5.3.1 - Rilevamento degli incidenti - Registrazione completa	Esiste una registrazione completa per supportare l'identificazione e la mitigazione degli incidenti?	Specificate se è abilitata la registrazione completa. Identifica i tipi di eventi che il sistema è in grado di registrare. Per quanto tempo vengono conservati i registri?	Sì. Vengono registrati i seguenti eventi: applicazioni, dispositivi e Servizi AWS simili e registri di flusso VPC. AWS CloudTrail I AWS Config I log vengono conservati per 1 anno.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	Gestione del rischio/risposta agli incidenti 5.3.2 - Rilevamento degli incidenti - Monitoraggio dei registri	Monitorate e segnalate attività insolite o sospette utilizzando i meccanismi di rilevamento come il monitoraggio dei log?	Specificate se vengono eseguiti regolarmente il monitoraggio e l'invio di avvisi di sicurezza. In caso affermativo, include il monitoraggio dei log per rilevare comportamenti insoliti o sospetti?	Sì. Tutti i log vengono monitorati per rilevare comportamenti insoliti, ad esempio più accessi non riusciti, accessi da una geolocalizzazione insolita o altri avvisi sospetti.
	Gestione del rischio/Risposta agli incidenti 5.3.3 - Rilevamento degli incidenti - Violazione dei dati di terze parti	Esiste un processo per identificare, rilevare e registrare i problemi di sicurezza, privacy o violazione dei dati dei subappaltatori?	Specificate se è in atto un processo per identificare e rilevare fornitori o subappaltatori di terze parti per violazioni dei dati, problemi di sicurezza o problemi di privacy.	Sì

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
SLA per la notifica degli incidenti	Gestione del rischio/risposta agli incidenti 5.4.1 - SLA per la notifica degli incidenti (richiede l'attestazione manuale)	Qual è lo SLA per l'invio di notifiche su incidenti o violazioni?	Qual è lo SLA per l'invio di notifiche relative a incidenti o violazioni?	7 giorni

Controlli delle politiche di sicurezza e configurazione

I controlli delle politiche di sicurezza e configurazione valutano le politiche di sicurezza e le configurazioni di sicurezza che proteggono gli asset di un'organizzazione. Questa tabella elenca i valori e le descrizioni per i controlli delle politiche di sicurezza e configurazione.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
Politiche per la sicurezza delle informazioni	Politica di sicurezza e configurazione 10.1.1 - Politiche per la sicurezza delle informazioni - Politica di sicurezza delle informazioni	Disponete di una politica di sicurezza delle informazioni di proprietà e gestita da un team addetto alla sicurezza?	Specificate se avete una politica di sicurezza delle informazioni. In caso affermativo, condividi o carica una prova manuale.	Sì. Costruiamo la nostra politica di sicurezza sulla base del framework NIST.
	Politica di sicurezza e configurazione 10.1.2 - Politiche	Tutte le politiche di sicurezza vengono riviste annualmente?	Specificate se le politiche di sicurezza vengono riviste	Sì. Revisionato ogni anno.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estrazione delle prove	Valore del campione
	per la sicurezza delle informazioni - Revisione delle politiche		annualmente. In caso negativo, con quale frequenza vengono riviste le politiche?	
Politiche per le configurazioni di sicurezza	Politica di sicurezza e configurazione 10.2.1 - Criteri per le configurazioni di sicurezza - Configurazioni di sicurezza (richiede l'attestazione manuale)	Gli standard di configurazione della sicurezza sono mantenuti e documentati?	Specificate se tutti gli standard di configurazione di sicurezza sono mantenuti e documentati. In caso affermativo, condividi o carica una prova manuale.	Sì
	Politica di sicurezza e configurazione 10.2.2 - Criteri per le configurazioni di sicurezza - Revisione delle configurazioni di sicurezza (richiede l'attestazione manuale)	Le configurazioni di sicurezza vengono riviste almeno una volta all'anno?	Specificate se le configurazioni di sicurezza vengono riviste almeno una volta all'anno. In caso negativo, specificare la frequenza di revisione.	Sì. Revisionato ogni 3 mesi.

Set di controlli	Titolo di controllo	Descrizione del controllo	Dettagli sull'estraneazione delle prove	Valore del campione
	Politica di sicurezza e configurazione 10.2.3 - Politiche per le configurazioni di sicurezza - Modifiche alle configurazioni	Le modifiche alle configurazioni vengono registrate?	Specificate se le modifiche alla configurazione vengono registrate. In caso affermativo, per quanto tempo vengono conservati i registri?	Sì. Tutte le modifiche alle configurazioni vengono monitorate e registrate. Gli avvisi vengono generati quando le configurazioni vengono modificate. I registri vengono conservati per 6 mesi.

Esportazione di istantanee come acquirente utilizzando Marketplace AWS

Informazioni sui fornitori

Un'istananea è un punto-in-time postura di un profilo di sicurezza. L'esportazione di istantanee offre un modo per scaricare e rivedere i dati offline, esaminare i dati relativi alle prove e confrontare i prodotti.

Esporta un'istananea

È possibile esportare nei formati JSON o CSV. Per esportare un'istananea, segui questi passaggi.

1. Accedere alla AWS Management Console e aprire la [console Marketplace AWS](#).
2. Scegli **Informazioni sui fornitori**.
3. Da **Informazioni sui fornitori**, scegli un prodotto.
4. Da **Sicurezza e conformità** scheda, vai al **Riepilogo** sezione, quindi scegli **Esporta**.
5. Dall'elenco a discesa, scegli **Scarica (JSON)** o **Scarica (CSV)**.

Controllo dell'accesso in Marketplace AWS Vendor Insights

AWS Identity and Access Management (IAM) è un servizio AWS che consente di controllare l'accesso alle risorse AWS. IAM è un servizio AWS il cui utilizzo non comporta costi aggiuntivi. Se sei un amministratore, puoi essere autenticato (accesso effettuato) e autorizzato (disporre di autorizzazioni) a utilizzare Marketplace AWS risorse. Marketplace AWS Vendor Insights utilizza IAM per controllare l'accesso ai dati del venditore, alle valutazioni, all'autoattestazione del venditore e ai report di audit standard del settore.

Il modo consigliato per controllare chi può fare cosa nel Portale di gestione Marketplace AWS è usare IAM per creare utenti e gruppi. Quindi aggiungi gli utenti ai gruppi e gestisci i gruppi. È possibile assegnare una politica o delle autorizzazioni al gruppo che forniscono autorizzazioni di sola lettura. Se hai altri utenti che richiedono l'accesso di sola lettura, puoi aggiungerli al gruppo che hai creato anziché aggiungere autorizzazioni ai loro Account AWS.

Una policy è un documento che definisce le autorizzazioni che si applicano a un utente, un gruppo o un ruolo. Le autorizzazioni determinano cosa possono fare gli utenti AWS. Una policy di solito consente l'accesso a operazioni specifiche e, facoltativamente, può garantire che le operazioni siano consentite per risorse specifiche, come istanze Amazon EC2, bucket Amazon S3. Le policy possono anche essere create per risorse specifiche. Un'autorizzazione è una dichiarazione all'interno di una policy che consente o nega l'accesso a una risorsa.

Important

Tutti gli utenti che crei si autenticano utilizzando le loro credenziali. Tuttavia, usano lo stesso Account AWS. Qualsiasi modifica apportata da un utente può influire sull'intero account.

Marketplace AWS ha delle autorizzazioni definite per controllare le azioni che può intraprendere qualcuno con tali autorizzazioni nel Portale di gestione Marketplace AWS. Esistono anche politiche che Marketplace AWS crea e gestisce che combinano diverse autorizzazioni. La politica `AWSMarketplaceSellerProductsFullAccess` offre all'utente l'accesso completo ai prodotti nel Portale di gestione Marketplace AWS.

Per ulteriori informazioni sulle operazioni, risorse e chiavi di condizione disponibili, consulta [Operazioni, risorse e chiavi di condizione per Marketplace AWS Vendor](#).

Autorizzazioni per gli acquirenti di Marketplace AWS Vendor Insights

È le autorizzazioni nelle policy IAM per Marketplace AWS Vendor Insights. Puoi combinare le autorizzazioni in un'unica politica IAM per concedere le autorizzazioni che desideri.

GetProfileAccessTerms

GetProfileAccessTerms consente agli utenti di recuperare i termini necessari per esaminare, accettare e accedere a un profilo Marketplace AWS Vendor Insights.

Gruppi di operazioni: di sola lettura e di lettura e di lettura e di lettura e di lettura e di

Risorse richieste: SecurityProfile.

ListEntitledSecurityProfiles

ListEntitledSecurityProfiles consente agli utenti di elencare tutti i profili di sicurezza che hanno il diritto attivo di leggere.

Gruppi di azioni: sola lettura, sola lista e lettura-scrittura.

Risorse richieste: Nessuno one one one one one

ListEntitledSecurityProfileSnapshots

ListEntitledSecurityProfileSnapshots consente agli utenti di elencare le istantanee del profilo di sicurezza per un profilo di sicurezza che hanno il diritto di leggere. SecurityProfile.

Gruppi di azioni: sola lettura, sola lista e lettura-scrittura.

Risorse richieste: SecurityProfile

GetEntitledSecurityProfileSnapshot

GetEntitledSecurityProfileSnapshot consente agli utenti di ottenere i dettagli di uno snapshot del profilo di sicurezza per un profilo di sicurezza che hanno il diritto di leggere.

Gruppi di operazioni: di sola lettura e di lettura e di lettura e di lettura e di lettura e di

Risorse richieste: SecurityProfile

Sicurezza attiva Marketplace AWS

Pubblichiamo software di venditori di alta qualità e lavoriamo attivamente per mantenere la qualità della nostra selezione. Poiché ogni cliente è diverso, il nostro obiettivo è fornire informazioni sufficienti sui prodotti elencati in Marketplace AWS modo che i clienti possano prendere buone decisioni di acquisto.

Note

Per informazioni sulla sicurezza dei prodotti di dati di AWS Data Exchange, consulta [Security](#) in the AWS Data Exchange User Guide.

Per informazioni sulla sicurezza per i venditori suMarketplace AWS, consulta la sezione [Marketplace AWSSicurezza](#) nella Guida del Marketplace AWS venditore.

Informazioni sugli abbonati condivise con i venditori

Potremmo condividere le tue informazioni di contatto con i nostri venditori per i seguenti motivi:

- Se è necessario che forniscano formazione ai clienti e supporto tecnico.
- Per l'attivazione del software, la configurazione e la personalizzazione dei contenuti.
- Compensa internamente i loro team di vendita.

Inoltre, possiamo condividere informazioni quali il nome dell'azienda, l'indirizzo completo e le tariffe di utilizzo con i venditori per consentire loro di compensare i propri team di vendita. Potremmo anche condividere determinate informazioni con i venditori per aiutarli a valutare l'efficacia delle loro campagne di marketing. I venditori possono utilizzare queste informazioni insieme a quelle già in loro possesso per determinare i premi per i propri team di vendita o l'utilizzo per un determinato acquirente.

Per il resto, generalmente non condividiamo le informazioni sui clienti con i venditori e tutte le informazioni condivise non consentono l'identificazione personale, a meno che l'utente non ci abbia autorizzato a condividere tali informazioni o riteniamo che fornire le informazioni ai venditori sia necessario per rispettare leggi o regolamenti.

Aggiorna le policy IAM a IPv6

Marketplace AWS i clienti utilizzano le politiche IAM per impostare un intervallo consentito di indirizzi IP e impedire a qualsiasi indirizzo IP al di fuori dell'intervallo configurato di accedere alle Marketplace AWS risorse.

Il dominio del Marketplace AWS sito Web è in fase di aggiornamento al protocollo IPv6.

Le policy di filtro degli indirizzi IP non aggiornate per la gestione degli indirizzi IPv6 potrebbero far perdere ai clienti l'accesso alle risorse del sito Marketplace AWS Web.

Clienti interessati dall'aggiornamento da IPv4 a IPv6

I clienti che utilizzano il doppio indirizzamento sono interessati da questo aggiornamento. Il dual-indirizzamento della rete supporta sia IPv4 che IPv6.

Se si utilizza il doppio indirizzamento, è necessario aggiornare le politiche IAM attualmente configurate con indirizzi in formato IPv4 per includere gli indirizzi in formato IPv6.

Per assistenza in caso di problemi di accesso, contatta [AWS Support](#).

Note

I seguenti clienti non sono interessati da questo aggiornamento:

- Clienti che utilizzano solo reti IPv4.
- Clienti che utilizzano solo reti IPv6.

Che cos'è IPv6?

IPv6 è lo standard IP di nuova generazione destinato a sostituire alla fine IPv4. La versione precedente, IPv4, utilizza uno schema di indirizzamento a 32 bit per supportare 4,3 miliardi di dispositivi. L'IPv6 utilizza invece l'indirizzamento a 128 bit per supportare circa 340 trilioni di trilioni di dispositivi (ovvero 2 alla 128esima potenza).

```
2001:cdba:0000:0000:0000:0000:3257:9652
```

```
2001:cdba:0:0:0:0:3257:9652
```

```
2001:cdba::3257:965
```


Aggiornamento di una policy IAM per IPv6

Le policy IAM vengono attualmente utilizzate per impostare un intervallo consentito di indirizzi IP utilizzando il `aws:SourceIp` filtro.

Il doppio indirizzamento supporta sia il traffico IPv4 che quello IPv6. Se la rete utilizzi un doppio indirizzamento, è necessario assicurarsi che le policy IAM utilizzate per il filtro degli indirizzi IP siano aggiornate per includere gli intervalli di indirizzi IPv6.

Ad esempio, questa policy dei bucket Amazon S3 identifica gli intervalli di indirizzi IPv4 consentiti `192.0.2.0.*` e `203.0.113.0.*` nell'elemento `Condition`.

```
# 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"
      }
    }
  }
}
```

Per aggiornare questa politica, l'elemento `Condition` della policy viene aggiornato per includere gli intervalli di indirizzi IPv6 `2001:DB8:1234:5678::/64` e `2001:cdba:3257:8593::/64`.

Note

NON RIMUOVERE gli indirizzi IPv4 esistenti perché sono necessari per la compatibilità con le versioni precedenti.

```

"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"
  }
}

```

Per ulteriori informazioni sulla gestione delle autorizzazioni di accesso con IAM, consulta [Politiche gestite e politiche in linea](#) nella Guida per l'AWS Identity and Access Management utente.

Test della rete dopo l'aggiornamento da IPv6 a IPv6

Dopo aver aggiornato le policy IAM al formato IPv6, puoi verificare se la tua rete sta accedendo all'endpoint IPv6 e alle funzionalità del Marketplace AWS sito Web.

Argomenti

- [Rete di test con Linux/Unix o Mac OS X](#)
- [Test della rete con Windows 7 o Windows 10](#)
- [Testare il Marketplace AWS sito web](#)

Rete di test con Linux/Unix o Mac OS X

Se utilizzi Linux/Unix o Mac OS X, puoi verificare se la rete accede all'endpoint IPv6 tramite il comando curl seguente.

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

Ad esempio, se la connessione è stata eseguita su IPv6, l'indirizzo IP connesso visualizza le informazioni seguenti.

```
* 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 della rete con Windows 7 o Windows 10

Se utilizzi Windows 7 o Windows 10, puoi verificare se la rete è in grado di accedere a un endpoint dual-stack su IPv4. Usa il comando ping come mostrato nell'esempio seguente.

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

Questo comando restituisce gli indirizzi IPv6 se si accede a un endpoint tramite IPv6.

Testare il Marketplace AWS sito web

Il test della funzionalità del Marketplace AWS sito Web dopo l'aggiornamento dipende principalmente da come è scritta la politica e da cosa viene utilizzata. In generale, è necessario verificare che la funzionalità specificata nella politica funzioni come previsto.

I seguenti scenari possono aiutarti a iniziare a testare la funzionalità del Marketplace AWS sito Web.

In qualità di acquirente sul Marketplace AWS sito web, verifica se è possibile eseguire le operazioni:

- Abbonati a un Marketplace AWS prodotto.
- Configura un Marketplace AWS prodotto.
- Lancia o realizza un Marketplace AWS prodotto.

In qualità di venditore sul Marketplace AWS sito web, verifica se è possibile eseguire le operazioni:

- Gestisci i tuoi Marketplace AWS prodotti esistenti.
- Crea un Marketplace AWS prodotto.

Controllo dell'accesso a Marketplace AWS sottoscrizioni

AWS IAM Identity Center ti aiuta a creare o connettere in modo sicuro le identità della tua forza lavoro e a gestirne l'accesso centralmente da tutte le parti Account AWS e applicazioni. IAM Identity

Center è l'approccio consigliato per l'autenticazione e l'autorizzazione della forza lavoro in AWS per organizzazioni di qualsiasi dimensione e tipo. Per ulteriori indicazioni sulla configurazione, consulta [il'Architettura di riferimento per la sicurezza AWS](#).

IAM Identity Center fornisce un portale utente in cui gli utenti possono trovare e accedere ai propri assegnati Account AWS, ruoli, applicazioni cloud e applicazioni personalizzate in un unico posto. IAM Identity Center assegna l'accesso Single Sign-On a utenti e gruppi nella directory connessa e utilizza set di autorizzazioni per determinarne il livello di accesso. Ciò abilita credenziali di sicurezza temporanee. È possibile definire il loro livello di accesso assegnando specifiche AWS ruoli gestiti per Marketplace AWS accesso per delegare la gestione di Marketplace AWS abbonamenti in tutto il tuo AWS organizzazione.

Ad esempio, il cliente A assume un ruolo tramite la federazione con `ManagedMarketplace_ViewOnly` politica associata al ruolo. Ciò significa che il cliente A può visualizzare gli abbonamenti solo in Marketplace AWS. Puoi creare un ruolo IAM con le autorizzazioni per visualizzare gli abbonamenti e concedere l'autorizzazione al cliente A per [assumi questo ruolo](#).

Creazione di ruoli IAM per Marketplace AWS accesso

Puoi utilizzare i ruoli IAM per delegare l'accesso alle risorse AWS.

Per creare ruoli IAM da assegnare Marketplace AWS autorizzazioni

1. Aprire la [console IAM](#).
2. Nel pannello di navigazione sinistro, scegli Roles (Ruoli), quindi Create role (Crea ruolo).
3. Scegli il tuo Account AWS.
4. Da Aggiungi autorizzazioni, seleziona una delle seguenti politiche:
 - Per consentire le autorizzazioni solo per visualizzare gli abbonamenti, ma non per modificarli, scegli `AWSMarketplaceRead-only`.
 - Per consentire le autorizzazioni di iscrizione e annullamento dell'iscrizione, scegli `AWSMarketplaceManageSubscriptions`.
 - Per consentire il controllo completo dei tuoi abbonamenti, scegli `AWSMarketplaceFullAccess`.
5. Seleziona Successivo.
6. Per Nome del ruolo, inserisci un nome per il ruolo. Ad esempio, *MarketplaceReadOnly* o *MarketplaceFullAccess*. Quindi seleziona Create role (Crea ruolo). Per ulteriori informazioni, vedere [Creazione di ruoli IAM](#).

Note

L'amministratore dell'account specificato può concedere l'autorizzazione di assumere questo ruolo a qualsiasi utente in tale account.

Ripeti i passaggi precedenti per creare più ruoli con set di autorizzazioni diversi in modo che ogni utente possa utilizzare il ruolo IAM con autorizzazioni personalizzate.

Non sei limitato alle autorizzazioni presenti in AWS politiche gestite che sono descritte qui. Puoi utilizzare IAM per creare policy con autorizzazioni personalizzate e quindi aggiungere tali policy ai ruoli IAM. Per ulteriori informazioni, consulta [Gestione delle politiche IAM](#) e [Aggiungere le autorizzazioni di identità IAM](#).

Policy gestite da AWS per Marketplace AWS

Puoi usare AWS politiche gestite per fornire informazioni di base Marketplace AWS autorizzazioni. Quindi, per ogni scenario unico, puoi creare le tue politiche e applicarle ai ruoli con i requisiti specifici per il tuo scenario. Le seguenti informazioni di base Marketplace AWS sono disponibili politiche gestite per controllare chi dispone di quali autorizzazioni:

- AWSMarketplaceRead-only
- AWSMarketplaceManageSubscriptions
- AWSPrivateMarketplaceRequests
- AWSPrivateMarketplaceAdminFullAccess
- AWSMarketplaceFullAccess

Marketplace AWS fornisce inoltre politiche gestite specializzate per scenari specifici. Per un elenco completo delle policy gestite da AWS per Marketplace AWS gli acquirenti, oltre alle descrizioni delle autorizzazioni che forniscono, consultano [AWS politiche gestite per Marketplace AWS gli acquirenti](#).

Autorizzazioni per l'utilizzo di License Manager

Marketplace AWS si integra con AWS License Manager per gestire e condividere le licenze dei prodotti a cui sottoscrivi un abbonamento tra gli account dell'organizzazione. Per visualizzare i dettagli completi dei tuoi abbonamenti in Marketplace AWS, un utente deve essere in grado di elencare le informazioni sulla licenza da AWS License Manager.

Per assicurarsi che i tuoi utenti dispongano delle autorizzazioni necessarie per visualizzare tutti i dati relativi ai loro Marketplace AWS prodotti e abbonamenti, aggiungi la seguente autorizzazione:

- `license-manager:ListReceivedLicenses`

Per ulteriori informazioni sull'impostazione delle autorizzazioni, vedere [Gestione delle politiche IAM](#) nel Guida per l'utente IAM.

Risorse aggiuntive

Per ulteriori informazioni sulla gestione dei ruoli IAM, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nel Guida per l'utente IAM.

Per ulteriori informazioni sulla gestione delle autorizzazioni e delle politiche IAM, consulta [Controllo dell'accesso a AWS risorse che utilizzano politiche](#) nel Guida per l'utente IAM.

Per ulteriori informazioni sulla gestione delle autorizzazioni e delle policy IAM per i prodotti di dati in AWS Data Exchange, consulta [Gestione delle identità e degli accessi in AWS Data Exchange](#) nel Guida per l'utente di AWS Data Exchange.

AWS politiche gestite per Marketplace AWS gli acquirenti

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Questa sezione elenca ciascuna delle politiche utilizzate per gestire l'accesso degli acquirenti a Marketplace AWS. Per informazioni sulle politiche del venditore, consulta [le politiche AWS gestite per Marketplace AWS i venditori](#) nella Guida al Marketplace AWS venditore.

Argomenti

- [AWSPolicy gestita: AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWSPolicy gestita: AWSMarketplaceFullAccess](#)
- [AWSpolitica gestita: AWSMarketplaceImageBuildFullAccess](#)
- [AWSpolitica gestita: AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWSpolitica gestita: AWSMarketplaceManageSubscriptions](#)
- [AWSpolitica gestita: AWSMarketplaceProcurementSystemAdminFullAccess](#)
- [AWSpolitica gestita: -only AWSMarketplaceRead](#)
- [AWSpolitica gestita: AWSPrivateMarketplaceAdminFullAccess](#)
- [AWSpolitica gestita: AWSPrivateMarketplaceRequests](#)
- [AWSPolicy gestita: AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWSPolicy gestita: AWSVendorInsightsAssessorFullAccess](#)
- [AWSPolicy gestita: AWSVendorInsightsAssessorReadOnly](#)
- [Aggiornamenti di Marketplace AWS alle policy gestite da AWS](#)

AWSPolicy gestita: AWSMarketplaceDeploymentServiceRolePolicy

Non è possibile collegare `AWSMarketplaceDeploymentServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Marketplace AWS di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Marketplace AWS](#).

Questa politica concede le autorizzazioni per i collaboratori che consentono di gestire i parametri relativi Marketplace AWS alla distribuzione, che sono archiviati come segreti in, per tuo conto. [AWS Secrets Manager](#)

AWSPolicy gestita: AWSMarketplaceFullAccess

È possibile allegare la policy `AWSMarketplaceFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ai servizi correlati, Marketplace AWS sia come acquirente che come venditore. Queste autorizzazioni

includono la possibilità di sottoscrivere e annullare l'iscrizione al Marketplace AWS software, gestire le istanze Marketplace AWS software dal Marketplace AWS, creare e gestire il marketplace privato nel proprio account, nonché l'accesso ad Amazon EC2 e Amazon EC2 Systems AWS CloudFormation Manager.

Dettagli dell'autorizzazione

```
{
  "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/*",
          ]
        }
      }
    }
  ],
  "Resource": [
    "*"
  ]
}

```



```

    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/marketplace-image-build:build-id": "*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/*Automation*",
      "arn:aws:iam::*:role/*Instance*"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:GetAutomationExecution",
      "ssm:ListDocuments",
      "ssm:DescribeDocument",
      "ec2:DeregisterImage",
      "ec2:CopyImage",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeImages",
      "ec2:DescribeSubnets",
      "ec2>DeleteSnapshot",
      "ec2>CreateImage",
      "ec2:RunInstances",
      "ec2:DescribeInstanceStatus",
      "sns:GetTopicAttributes",
      "iam:GetRole",
      "iam:GetInstanceProfile"
    ],
    "Resource": "*"
  },

```

```

{
  "Effect": "Allow",
  "Action": [
    "ssm:StartAutomationExecution"
  ],
  "Resource": [
    "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
    "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
    "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
    "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
    "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
    "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
    "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
    "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3::*image-build*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags"
  ],
  "Resource": [
    "arn:aws:ec2::*:image/*",
    "arn:aws:ec2::*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "sns:Publish"
  ],
  "Resource": [
    "arn:aws:sns::*:*image-build*"
  ]
}

```

```

    }
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "iam:PassedToService": [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN": [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:RequestTag/marketplace-image-build:build-id": "*"
        },
        "StringNotEquals": {
          "ec2:CreateAction": "RunInstances"
        }
      }
    }
  }
}

```

```
]
}
```

AWSpolitica gestita:

AWSMarketplaceLicenseManagementServiceRolePolicy

Non puoi collegarti AWSMarketplaceLicenseManagementServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Marketplace AWS di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Marketplace AWS](#).

Questa politica concede le autorizzazioni per i contributori che consentono di gestire le licenze Marketplace AWS per tuo conto.

Dettagli dell'autorizzazione

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

AWSpolitica gestita: AWSMarketplaceManageSubscriptions

È possibile allegare la policy AWSMarketplaceManageSubscriptions alle identità IAM.

Questa politica concede ai contributori le autorizzazioni che consentono la sottoscrizione e l'annullamento dell'iscrizione ai prodotti. Marketplace AWS

Dettagli dell'autorizzazione

```
{
  "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"
      ]
    }
  ]
}
```


AWSpolitica gestita: AWSMarketplaceProcurementSystemAdminFullAccess

È possibile allegare la policy `AWSMarketplaceProcurementSystemAdminFullAccess` alle identità IAM.

Questa politica concede le autorizzazioni di amministratore che consentono di gestire tutti gli aspetti di un'integrazione di Marketplace AWS eProcurement, inclusa l'elencazione degli account dell'organizzazione. Per ulteriori informazioni sulle integrazioni di eProcurement, consulta.

[Integrazione Marketplace AWS con i sistemi di approvvigionamento](#)

Dettagli dell'autorizzazione

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

AWSpolitica gestita: -only AWSMarketplaceRead

È possibile allegare la policy `AWSMarketplaceRead-only` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono di visualizzare prodotti, offerte private e abbonamenti per il tuo account Marketplace AWS, oltre a visualizzare le risorse Amazon EC2 AWS Identity and Access Management e Amazon SNS nell'account.

Dettagli dell'autorizzazione

```
{
  "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 politica gestita: AWSPrivateMarketplaceAdminFullAccess

È possibile allegare la policy AWSPrivateMarketplaceAdminFullAccess alle identità IAM.

Questa politica concede le autorizzazioni di amministratore che consentono l'accesso completo alla gestione dei marketplace privati nel tuo account (o organizzazione). Per ulteriori informazioni sull'utilizzo di più amministratori, consulta [the section called "Creazione di politiche personalizzate per gli amministratori del marketplace privato"](#)

Dettagli dell'autorizzazione

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

```

AWSPolitica gestita: AWSPPrivateMarketplaceRequests

È possibile allegare la policy AWSPPrivateMarketplaceRequests alle identità IAM.

Questa politica concede le autorizzazioni dei contributori che consentono l'accesso alla richiesta di aggiunta di prodotti al tuo marketplace privato e alla visualizzazione di tali richieste. Queste richieste devono essere approvate o rifiutate da un amministratore privato del marketplace.

Dettagli dell'autorizzazione

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```
{
  "Effect": "Allow",
  "Action": [
    "aws-marketplace:CreatePrivateMarketplaceRequests",
    "aws-marketplace:ListPrivateMarketplaceRequests",
    "aws-marketplace:DescribePrivateMarketplaceRequests"
  ],
  "Resource": "*"
}
```

AWSPolicy gestita: AWSServiceRoleForPrivateMarketplaceAdminPolicy

Non è possibile collegare `AWSServiceRoleForPrivateMarketplaceAdminPolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Marketplace AWS di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Marketplace AWS](#).

Questa politica concede le autorizzazioni Marketplace AWS per i contributori che consentono di descrivere e aggiornare le risorse di Private Marketplace e descrivere. AWS Organizations

AWSPolicy gestita: AWSVendorInsightsAssessorFullAccess

È possibile allegare la policy `AWSVendorInsightsAssessorFullAccess` alle identità IAM.

Questa politica garantisce l'accesso completo alla visualizzazione delle risorse Vendor Insights autorizzate e alla gestione degli abbonamenti a Marketplace AWS Vendor Insights. Marketplace AWS Queste richieste devono essere approvate o rifiutate da un amministratore. Consente l'accesso in sola lettura ai report di AWS Artifact terze parti.

Marketplace AWS Vendor Insights identifica che il valutatore è uguale all'acquirente e il fornitore è uguale al venditore.

Dettagli dell'autorizzazione

```
{
  "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/*"
  }
]
}

```

AWSPolicy gestita: AWSVendorInsightsAssessorReadOnly

È possibile allegare la policy `AWSVendorInsightsAssessorReadOnly` alle identità IAM.

Questa politica garantisce l'accesso in sola lettura per la visualizzazione delle risorse di Vendor Insights autorizzate. Marketplace AWS Queste richieste devono essere approvate o rifiutate da un amministratore. Consente l'accesso in sola lettura ai report in. AWS Artifact

le richieste devono essere approvate o rifiutate da un amministratore. Consente l'accesso in sola lettura ai report di AWS Artifact terze parti.

Marketplace AWS Ai fini di questa guida, Vendor Insights identifica come valutatore l'acquirente e il venditore è uguale al venditore.

Dettagli dell'autorizzazione

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

Aggiornamenti di Marketplace AWS alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per Marketplace AWS da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche

apportate a questa pagina, sottoscrivere il feed RSS nella pagina [Cronologia dei documenti](#) di Marketplace AWS

Modifica	Descrizione	Data
AWSServiceRoleForPrivateMarketplaceAdminPolicy — È stata aggiunta una politica per nuove funzionalità in Marketplace AWS	Marketplace AWS ha aggiunto una nuova politica per supportare la gestione e la descrizione AWS Organizations delle risorse di Private Marketplace.	16 febbraio 2024
AWSPrivateMarketplaceAdminFullAccess : aggiornamento a policy esistente	Marketplace AWS ha aggiornato la politica per supportare la lettura AWS Organizations dei dati.	16 febbraio 2024
AWSMarketplaceDeploymentServiceRolePolicy — Aggiunta politica per nuove funzionalità in Marketplace AWS	Marketplace AWS ha aggiunto una nuova policy per supportare la gestione dei parametri relativi alla distribuzione.	29 novembre 2023
AWSMarketplaceReadSolo e — aggiornamenti alle politiche esistenti AWSMarketplaceManageSubscriptions	Marketplace AWS ha aggiornato le politiche esistenti per consentire l'accesso alla pagina delle offerte private.	19 gennaio 2023
AWSPrivateMarketplaceAdminFullAccess : aggiornamento a policy esistente	Marketplace AWS ha aggiornato la politica per la nuova funzionalità di autorizzazione basata su tag.	9 dicembre 2022
AWSVendorInsightsAssessorReadOnly Marketplace AWS aggiornato AWSVendorInsightsAssessorReadOnly	Marketplace AWS aggiornato AWSVendorInsightsAssessorReadOnly per aggiungere l'accesso in sola lettura ai report nei report	30 novembre 2022

Modifica	Descrizione	Data
	AWS Artifact di terze parti (anteprima).	
AWSVendorInsightsAssessorFullAccess Marketplace AWSaggiornato AWSVendorInsightsAssessorFullAccess	Marketplace AWSaggiornato AWSVendorInsightsAssessorFullAccess per aggiungere la ricerca di accordi e l'accesso in sola lettura al rapporto di AWS Artifact terze parti (anteprima).	30 novembre 2022
AWSVendorInsightsAssessorFullAccess AWSVendorInsightsAssessorReadOnly — Sono state aggiunte politiche per nuove funzionalità in Marketplace AWS	Marketplace AWSpolitiche che aggiunte per la nuova funzionalità Marketplace AWS Vendor Insights: AWSVendorInsightsAssessorFullAccess e AWSVendorInsightsAssessorReadOnly	26 luglio 2022
AWSMarketplaceFullAccess AWSMarketplaceImageBuildFullAccess — Aggiornamenti a una politica esistente	Marketplace AWSha rimosso le autorizzazioni non più necessarie per migliorare la sicurezza.	4 marzo 2022
AWSPrivateMarketplaceAdminFullAccess : aggiornamento a una policy esistente	Marketplace AWSle autorizzazioni non utilizzate sono state rimosse nella politica. AWSPrivateMarketplaceAdminFullAccess	27 agosto 2021

Modifica	Descrizione	Data
AWSMarketplaceFullAccess : aggiornamento a una policy esistente	Marketplace AWS ha rimosso un'ec2:DescribeAccountAttributes autorizzazione duplicata dalla politica. AWSMarketplaceFullAccess	20 luglio 2021
Marketplace AWS ha iniziato il rilevamento delle modifiche	Marketplace AWS ha iniziato il rilevamento delle modifiche per le relative policy gestite da AWS.	20 aprile 2021

Individuazione dell'Account AWS numero per l'assistenza clienti

Se tu o i tuoi utenti avete bisogno di contattare AWS Support, avete bisogno del vostro Account AWS numero.

Per trovare il tuo Account AWS numero

1. Accedi [AWS Management Console](#) con il tuo nome utente.
2. Nella barra di navigazione in alto, scegli Support, quindi scegli Support Center.

Il tuo Account AWS ID (numero di conto) viene visualizzato sotto la barra di navigazione in alto.

Utilizzo di ruoli collegati ai servizi per Marketplace AWS

Marketplace AWS utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Marketplace AWS. I ruoli collegati ai servizi sono definiti automaticamente da Marketplace AWS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Argomenti

- [Utilizzo dei ruoli per condividere i diritti per Marketplace AWS](#)
- [Utilizzo dei ruoli per gestire gli ordini di acquisto in Marketplace AWS](#)

- [Utilizzo dei ruoli per configurare e lanciare prodotti in Marketplace AWS](#)
- [Utilizzo dei ruoli per configurare Private Marketplace in Marketplace AWS](#)

Utilizzo dei ruoli per condividere i diritti per Marketplace AWS

Marketplace AWS utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Marketplace AWS. I ruoli collegati ai servizi sono definiti automaticamente da Marketplace AWS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione Marketplace AWS perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Marketplace AWS definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. Marketplace AWS Le autorizzazioni definite includono policy di attendibilità e di autorizzazioni. Questa policy delle autorizzazioni non può essere collegata ad alcun'altra entità IAM.

Per condividere le Marketplace AWS sottoscrizioni ad altri account AWS dell'organizzazione AWS License Manager, è necessario concedere Marketplace AWS le autorizzazioni per ogni account con cui si desidera condividere. A tale scopo, utilizzare il ruolo `AWSServiceRoleForMarketplaceLicenseManagement`. Per ulteriori dettagli, consulta [Creazione di un ruolo collegato ai servizi per Marketplace AWS](#).

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWSi servizi che funzionano con IAM](#) e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli un Sì con un link per visualizzare la documentazione del ruolo collegato al servizio per quel servizio.

Autorizzazioni del ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS usa il ruolo collegato ai servizi denominato `AWSServiceRoleForMarketplaceLicenseManagement`. Questo ruolo fornisce Marketplace AWS le autorizzazioni per creare e gestire le licenze AWS License Manager per i prodotti a cui ti abboni. Marketplace AWS

Il ruolo `AWSServiceRoleForMarketplaceLicenseManagement` collegato al servizio affida al seguente servizio l'esecuzione di azioni in License Manager per conto dell'utente:

- `license-management.marketplace.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSMarketplaceLicenseManagementServiceRolePolicy` consente di Marketplace AWS completare le seguenti azioni sulle risorse specificate:

- Operazioni:
 - `"organizations:DescribeOrganization"`
 - `"license-manager:ListReceivedGrants"`
 - `"license-manager:ListDistributedGrants"`
 - `"license-manager:GetGrant"`
 - `"license-manager:CreateGrant"`
 - `"license-manager:CreateGrantVersion"`
 - `"license-manager>DeleteGrant"`
 - `"license-manager:AcceptGrant"`
- Risorse:
 - Tutte le risorse () `"*"`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei ruoli collegati ai servizi](#) nella Guida per l'utente IAM.

Creazione di un ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS crea automaticamente il ruolo collegato al servizio quando configuri l'integrazione con AWS License Manager.

È possibile specificare di Marketplace AWS creare il ruolo collegato al servizio per tutti gli account dell'organizzazione contemporaneamente oppure è possibile creare il ruolo collegato al servizio per un account alla volta. L'opzione per creare ruoli collegati al servizio per tutti gli account è disponibile solo se l'organizzazione ha tutte le funzionalità abilitate. Per maggiori dettagli, consulta [Attivazione di tutte le funzionalità nell'organizzazione nella Guida](#) per l'AWS Organizations utente.

Per creare ruoli collegati ai servizi in tutti gli account

1. Nella [Marketplace AWS console](#), accedi e scegli Impostazioni.
2. Nella sezione AWS Organizations integrazione, seleziona Crea integrazione.

3. Nella pagina Crea AWS Organizations integrazione, seleziona Abilita l'accesso affidabile in tutta l'organizzazione, quindi scegli Crea integrazione.

Note

Questa impostazione abilita la fiducia interna AWS Organizations. Di conseguenza, oltre all'azione corrente, agli account futuri aggiunti all'organizzazione viene aggiunto automaticamente il ruolo collegato al servizio.

Per creare ruoli collegati al servizio per l'account corrente

1. Nella [Marketplace AWS console](#), accedi e scegli Impostazioni.
2. Nella sezione AWS Organizations integrazione, seleziona Configura integrazione.
3. Nella pagina Crea AWS Organizations integrazione, seleziona il ruolo collegato al servizio di gestione delle Marketplace AWS licenze per questo account, quindi scegli Crea integrazione.

Important

Se scegli di creare il ruolo collegato al servizio solo per l'account corrente, ciò non consente l'accesso affidabile all'interno dell'organizzazione. È necessario ripetere questi passaggi per ogni account con cui si desidera condividere (dare o ricevere) licenze. Marketplace AWS Ciò include gli account che verranno aggiunti all'organizzazione in futuro.

Modifica di un ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS non consente di modificare il ruolo collegato ai servizi. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio nella Guida](#) per l'utente IAM.

Eliminazione di un ruolo collegato ai servizi per Marketplace AWS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Note

Se il servizio Marketplace AWS utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi `AWSServiceRoleForMarketplaceLicenseManagement`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Marketplace AWS

Marketplace AWS supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni AWS in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di Marketplace AWS](#).

Utilizzo dei ruoli per gestire gli ordini di acquisto in Marketplace AWS

Marketplace AWS utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#).

Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Marketplace AWS. I ruoli collegati ai servizi sono definiti automaticamente da Marketplace AWS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Marketplace AWS perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Marketplace AWS definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, Marketplace AWS potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Marketplace AWS perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForMarketplacePurchaseOrders`: questo ruolo fornisce Marketplace AWS le autorizzazioni per allegare i numeri degli ordini di acquisto Marketplace AWS agli abbonamenti in AWS Billing and Cost Management.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForMarketplacePurchaseOrders` considera attendibili i seguenti servizi:

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

La politica di autorizzazione dei ruoli denominata `AWSMarketplacePurchaseOrdersServiceRolePolicy` consente di Marketplace AWS completare le seguenti azioni sulle risorse specificate:

- Operazione: `"purchase-orders:ViewPurchaseOrders"`, `"purchase-orders:ModifyPurchaseOrders"` su `"*"`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Marketplace AWS

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando configuri l'integrazione con AWS Billing and Cost Management, Marketplace AWS crea automaticamente il ruolo collegato al servizio.

Note

All'interno AWS Organizations, questa impostazione funziona solo nell'account di gestione. È necessario eseguire questa procedura dall'account di gestione. Questo imposta il ruolo collegato al servizio e il supporto per gli ordini di acquisto per tutti gli account dell'organizzazione.

Come creare un ruolo collegato a un servizio

1. Nella [Marketplace AWSconsole](#), accedi all'account di gestione e scegli Impostazioni.
2. Nella sezione AWSIntegrazione della fatturazione, seleziona Configura integrazione.
3. Nella pagina di integrazione Crea AWS fatturazione, seleziona il ruolo collegato al servizio di gestione della Marketplace AWS fatturazione per la tua organizzazione, quindi scegli Crea integrazione.

Se devi ricreare un ruolo collegato ai servizi che hai precedentemente eliminato, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando configuri l'integrazione conAWS Billing and Cost Management, Marketplace AWS crea nuovamente il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForMarketplacePurchaseOrders`. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Marketplace AWS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Eliminazione manuale del ruolo collegato al servizio

Utilizzare la console IAM, AWS CLI, la AWS o l'API per eliminare i ruoli collegati ai servizi `AWSServiceRoleForMarketplacePurchaseOrders`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Marketplace AWS

Marketplace AWS supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni AWSin cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di Marketplace AWS](#).

Utilizzo dei ruoli per configurare e lanciare prodotti in Marketplace AWS

Marketplace AWS utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Marketplace AWS. I ruoli collegati ai servizi sono definiti automaticamente da Marketplace AWS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Marketplace AWS perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Marketplace AWS definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, Marketplace AWS potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForMarketplaceDeployment` per consentire la gestione dei parametri relativi Marketplace AWS alla distribuzione, archiviati come segreti in, per conto dell'utente. [AWS Secrets Manager](#) I venditori possono fare riferimento a questi segreti nei AWS CloudFormation modelli, che puoi avviare durante la configurazione di prodotti su cui è abilitato Quick Launch. Marketplace AWS

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForMarketplaceDeployment` considera attendibili i seguenti servizi:

- `deployment.marketplace.amazonaws.com`

Utilizza la politica di autorizzazione dei ruoli denominata `AWSMarketplaceDeploymentServiceRolePolicy` per consentire il Marketplace AWS completamento delle azioni sulle tue risorse.

Note

Per ulteriori informazioni sulle policy Marketplace AWS gestite, consulta le [policy gestite di AWS per Marketplace AWS gli acquirenti](#).

```

{
  "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}"
}
}
]
}
```

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Marketplace AWS

La configurazione del ruolo collegato al servizio è un'azione unica che fornisce le autorizzazioni per tutti i prodotti su cui è abilitato Quick Launch, purché il ruolo esista.

Quando configuri un prodotto con Quick Launch abilitato, Marketplace AWS rileva se hai creato il ruolo collegato al servizio richiesto per il tuo account. Se il ruolo è mancante, viene visualizzato un messaggio per abilitare l'integrazione dei parametri di Marketplace AWS distribuzione, che include un pulsante **Abilita integrazione**. Marketplace AWS crea automaticamente il ruolo collegato al servizio quando si seleziona questo pulsante.

Important

Questo ruolo collegato al servizio verrà visualizzato nel tuo account se in precedenza hai configurato un prodotto con Quick Launch abilitato. Per ulteriori informazioni, vedi [A new role appeared in my](#). Account AWS

Se elimini questo ruolo collegato al servizio e devi crearlo di nuovo, puoi utilizzare la stessa procedura per ricreare il ruolo nel tuo account. Quando apri la pagina di configurazione per qualsiasi prodotto con Quick Launch abilitato, vedrai il pulsante **Abilita integrazione**, che puoi scegliere nuovamente per ricreare il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM per creare un ruolo collegato ai servizi con lo use case AWS Marketplace - Deployment Management. In AWS CLI o in AWS API, crea un ruolo collegato al servizio con il nome di servizio `deployment.marketplace.amazonaws.com`. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS non consente di modificare il ruolo collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Marketplace AWS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Note

Se il servizio utilizza il ruolo quando si tenta di eliminarlo, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare Marketplace AWS le risorse utilizzate dal `deployment.marketplace.amazonaws.com` servizio, devi eliminare tutti i segreti relativi a Marketplace Deployment da SecretsManager. Puoi trovare i segreti pertinenti nei seguenti modi:

- Ricerca di segreti gestiti da `marketplace-deployment`.
- Alla ricerca di segreti con i tag `key aws:secretsmanager:owningService and valuemarketplace-deployment`.
- Ricerca di segreti il cui nome è preceduto da `marketplace-deployment!`.

Per eliminare il ruolo collegato al servizio utilizzando IAM

Utilizzare la console IAM, AWS CLI, la AWS o l'API per eliminare i ruoli collegati ai servizi `AWSServiceRoleForMarketplaceDeployment`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Marketplace AWS

Marketplace AWS supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [AWS Marketplace Regions and Endpoints](#).

Utilizzo dei ruoli per configurare Private Marketplace in Marketplace AWS

Marketplace AWS utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Marketplace AWS. I ruoli collegati ai servizi sono definiti automaticamente da Marketplace AWS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Marketplace AWS perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Marketplace AWS definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, Marketplace AWS potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta [Servizi AWS che funzionano con IAM](#) e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForPrivateMarketplaceAdmin` per descrivere e aggiornare le risorse e descrivere di Private Marketplace. AWS Organizations

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForPrivateMarketplaceAdmin` considera attendibili i seguenti servizi:

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

Utilizza la politica di autorizzazione dei ruoli denominata `AWSServiceRoleForPrivateMarketplaceAdminPolicy` per consentire di Marketplace AWS eseguire le seguenti azioni su risorse specifiche.

Note

Per ulteriori informazioni sulle policy gestite di AWS Marketplace, consulta le [policy gestite di AWS per Marketplace AWS gli acquirenti](#).

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

```

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Marketplace AWS

Non devi creare manualmente il ruolo collegato al servizio . Quando abiliti Private Marketplace per la tua organizzazione, Marketplace AWS crea il ruolo collegato al servizio per te.

Note

Questo ruolo è richiesto solo nell'account di gestione di AWS Organizations e viene creato solo nell'account di gestione.

Come creare un ruolo collegato a un servizio

1. Nella pagina Guida introduttiva a Private Marketplace, seleziona le opzioni per abilitare l'accesso affidabile in tutta l'organizzazione e creare un ruolo collegato al servizio Private Marketplace. Queste opzioni sono disponibili solo per l'account di gestione.
2. Scegli Abilita Private Marketplace.

Se sei già cliente di Private Marketplace, le opzioni per abilitare l'accesso affidabile all'interno dell'organizzazione e abilitare un ruolo collegato al servizio Private Marketplace saranno disponibili nella pagina Impostazioni della dashboard amministrativa del tuo marketplace privato.

Se elimini questo ruolo collegato al servizio e devi crearlo di nuovo, puoi utilizzare la stessa procedura per ricreare il ruolo nel tuo account.

Modifica di un ruolo collegato ai servizi per Marketplace AWS

Marketplace AWS non consente di modificare il ruolo collegato ai servizi. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Marketplace AWS

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Prima di poter eliminare il ruolo collegato al servizio, devi:

- Disabilita l'accesso affidabile in tutta l'organizzazione.
- Dissocia tutte le esperienze di mercato private.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi `AWSServiceRoleForPrivateMarketplaceAdmin`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Marketplace AWS

Marketplace AWS supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [AWS Marketplace Regions and Endpoints](#).

Creazione di un amministratore del marketplace privato

Puoi creare un gruppo di amministratori per gestire le impostazioni del [marketplace privato](#) della tua azienda. Dopo aver abilitato il marketplace privato per la tua organizzazione, gli amministratori del marketplace privato possono eseguire molte attività, tra cui:

- Visualizza e crea esperienze e destinatari.
- Aggiungi prodotti alle esperienze di marketplace private.
- Rimuovi i prodotti dalle esperienze di marketplace private.
- Configura l'interfaccia utente delle esperienze di marketplace private.
- Abilita e disabilita le esperienze di marketplace private.
- Chiamali AWS Marketplace Catalog API per gestire le esperienze di mercato private in modo programmatico.

Per creare più amministratori di marketplace privati in cui ogni amministratore è limitato a un sottoinsieme di attività, consulta [the section called "Creazione di politiche personalizzate per gli amministratori del marketplace privato"](#)

Note

L'attivazione del marketplace privato è un'azione una tantum che deve essere eseguita dall'account di gestione. Per ulteriori informazioni, consulta [Guida introduttiva a Private Marketplace](#).

Concedi AWS Identity and Access Management (IAM) le autorizzazioni per amministrare il tuo marketplace privato associandolo [the section called “AWSPrivateMarketplaceAdminFullAccess”](#) a un utente, gruppo o ruolo. Ti consigliamo di utilizzare un gruppo o un ruolo. Per ulteriori informazioni su come allegare la policy, consulta [Allegare una policy a un gruppo di utenti](#) nella IAM User Guide.

Per ulteriori informazioni sulle autorizzazioni contenute nella `AWSPrivateMarketplaceAdminFullAccess` policy, consulta [the section called “AWSPrivateMarketplaceAdminFullAccess”](#). Per ulteriori informazioni sulle altre politiche da utilizzare Marketplace AWS, accedi a e vai alla [pagina delle politiche IAM](#). AWS Management Console
Nella casella di ricerca, inserisci **Marketplace** per trovare tutte le politiche associate a Marketplace AWS.

Creazione di politiche personalizzate per gli amministratori del marketplace privato

La tua organizzazione può creare più amministratori di marketplace privati in cui ogni amministratore è limitato a un sottoinsieme di attività. Puoi ottimizzare le policy AWS Identity and Access Management (IAM) per specificare le chiavi e le risorse delle condizioni sulle AWS Marketplace Catalog API azioni elencate in [Azioni, risorse e chiavi di condizione per Marketplace AWS](#) Catalog. Il meccanismo generale per utilizzare i tipi di AWS Marketplace Catalog API modifica e le risorse per ottimizzare le politiche IAM è descritto nella [guida all'API AWS Marketplace Catalog](#). Per un elenco di tutti i tipi di modifica disponibili in modalità privata Marketplace AWS, consulta [Lavorare con un marketplace privato](#).

Per creare politiche gestite dai clienti, consulta [Creazione di politiche IAM](#). Di seguito è riportato un esempio di policy JSON che puoi utilizzare per creare un amministratore che può aggiungere o rimuovere prodotti solo dai marketplace privati.

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

```

Una policy può anche essere limitata alla gestione di un sottoinsieme di risorse private del marketplace. Di seguito è riportato un esempio di policy JSON che puoi utilizzare per creare un

amministratore che può gestire solo una specifica esperienza di marketplace privato. Questo esempio utilizza una stringa di risorse con `exp-1234example` come Experience identificatore.

```
{
  "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"
      ]
    }
  ]
}
```

Per informazioni dettagliate su come recuperare gli identificatori di entità e per visualizzare il set di risorse del marketplace privato, consulta [Lavorare con un marketplace privato](#).

Cronologia dei documenti

La tabella seguente descrive la documentazione per questa versione della Guida Marketplace AWS all'acquisto.

Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi iscriverti al feed RSS.

Modifica	Descrizione	Data
Politica di supporto AWS Organizations aggiornata	Politica gestita aggiornata <code>AWSPriVateMarketpl aceAdminFullAccess</code> per consentire l'accesso ai AWS Organizations dati di lettura.	16 febbraio 2024
Nuovo ruolo legato ai servizi per i prodotti in Marketplace AWS	Marketplace AWSora fornisce un ruolo collegato al servizio per descrivere e aggiornare le risorse e descrivere di Private Marketplace. AWS Organizat ions	16 febbraio 2024
Nuova esperienza di mercato privato su Marketplace AWS	Marketplace AWSora supporta l'integrazione AWS Organizat ions e la possibilità di registrar e amministratori delegati per amministrare esperienze di marketplace private.	16 febbraio 2024
Disponibilità generale per contratti con date future in Marketplace AWS	La funzionalità degli accordi con data futura per tutti gli ISV SaaS e i Channel Partner è ora generalmente disponibile in. Marketplace AWS Utilizzan do accordi con date future, i clienti possono prenotare in	16 gennaio 2024

	anticipo le offerte o impostare i rinnovi quando hanno già acquistato lo stesso elenco di prodotti con uno sforzo operativo ridotto.	
Supporto per la regione Canada occidentale (Calgary)	Marketplace AWS ora supporta quanto segue Regione AWS: Canada West (Calgary).	20 dicembre 2023
Nuovo ruolo legato ai servizi per i prodotti in Marketplace AWS	Marketplace AWS ora fornisce un ruolo collegato ai servizi per gestire i parametri relativi all'implementazione, che vengono archiviati come segreti per conto degli acquirenti. AWS Secrets Manager	29 novembre 2023
Nuova opzione di implementazione Quick Launch per gli acquirenti	Gli acquirenti possono ora ridurre il tempo, le risorse e i passaggi necessari per configurare, implementare e lanciare prodotti SaaS (Software as a Service) applicabili in Marketplace AWS	29 novembre 2023
Per le offerte private sono disponibili piani di pagamento flessibili	Gli orari di pagamento flessibili (FPS) per le offerte private sono ora disponibili per tutti i clienti di Marketplace AWS.	17 novembre 2023
Componenti aggiuntivi di terze parti di Amazon EKS	I clienti possono ora abbonarsi a componenti aggiuntivi di terze parti dalla console Amazon EKS senza essere reindirizzati. Marketplace AWS	18 ottobre 2023

Support per Amazon EventBridge	Marketplace AWS è ora integrato con Amazon EventBridge, precedentemente chiamato Amazon CloudWatch Events.	6 settembre 2023
Support per la regione di Israele (Tel Aviv)	Marketplace AWS ora supporta quanto segue Regione AWS: Israele (Tel Aviv).	1° agosto 2023
Supporto agli ordini di acquisto per i contratti annuali AMI	Marketplace AWS ora supporta la funzionalità degli ordini di acquisto per i contratti annuali di Amazon Machine Image (AMI).	29 giugno 2023
Disponibilità degli ordini di acquisto nella AWS Billing console	Gli acquirenti possono ora gestire tutti i loro ordini di acquisto nella AWS Billing console e riconciliare facilmente le fatture PDF del contratto out-of-cycle SaaS con gli ordini di acquisto corrispondenti.	3 febbraio 2023
Supporto per la regione Asia Pacifico (Melbourne)	Marketplace AWS ora supporta quanto segue Regione AWS: Asia Pacifico (Melbourne).	24 gennaio 2023
Politiche aggiornate per la pagina delle offerte private	Politiche gestite aggiornate e AWS Marketplace Read-only e AWS Marketplace Manage Subscriptions per consentire l'accesso alla pagina delle offerte private.	19 gennaio 2023

Pagina delle offerte private	Gli acquirenti autenticati possono ora visualizzare le offerte Marketplace AWS private estese a loro nella Account AWS pagina delle offerte private.	19 gennaio 2023
Notifiche e-mail aggiornate per gli acquirenti	Gli acquirenti vengono ora avvisati quando viene pubblicata un'offerta privata.	22 dicembre 2022
Le versioni di prova gratuite SaaS per gli abbonamenti sono ora disponibili per gli acquirenti su Marketplace AWS	Gli acquirenti possono ora abbonarsi a prove gratuite per i prodotti SaaS in abbonamento.	16 dicembre 2022
Gli acquirenti possono accettare un aggiornamento o un rinnovo di un'offerta privata SaaS	Se un venditore ha aggiornato o rinnovato una precedente offerta privata SaaS, gli acquirenti possono accettare una nuova offerta privata senza dover annullare il contratto esistente.	13 dicembre 2022
Marketplace AWS supporta l'archiviazione delle esperienze e dei marketplace privati	Gli acquirenti possono ora archiviare e riattivare le esperienze dei marketplace privati in Marketplace AWS	12 dicembre 2022
Politica aggiornata per la funzionalità di autorizzazione Marketplace AWS basata su tag	È stata aggiornata la <code>AWSPrivateMarketplaceAdminFullAccess</code> politica per supportare l'autorizzazione basata su tag in Marketplace AWS	9 dicembre 2022

<u>È stato aggiunto un nuovo argomento che fornisce informazioni su come annullare l'abbonamento</u>	Sono state aggiunte informazioni su come annullare l'abbonamento ai prodotti AMI, ML e SaaS in. Marketplace AWS Inoltre, sono state aggiunte informazioni sull'annullamento del rinnovo automatico per un contratto SaaS.	8 dicembre 2022
<u>Politiche aggiornate per gli acquirenti in Vendor Insights Marketplace AWS</u>	Politiche gestite aggiornate e AWSVendorInsightsAssessorFullAccess e AWSVendorInsightsAssessorReadOnly per gli acquirenti di Marketplace AWS Vendor Insights.	30 novembre 2022
<u>Controllo dell'accesso per gli acquirenti in Marketplace AWS Vendor Insights</u>	È stato aggiunto un nuovo argomento in Marketplace AWS Vendor Insights per descrivere le azioni e le autorizzazioni disponibili per gli acquirenti.	30 novembre 2022
<u>Supporto per la regione Asia Pacifico (Hyderabad)</u>	Marketplace AWS ora supporta quanto segue Regione AWS: Asia Pacifico (Hyderabad).	22 novembre 2022
<u>Supporto per la regione Europa (Spagna)</u>	Marketplace AWS ora supporta quanto segue Regione AWS: Europa (Spagna).	16 novembre 2022
<u>Support for Europe (Zurich) Region</u>	Marketplace AWS ora supporta quanto segue Regione AWS: Europa (Zurigo).	9 novembre 2022

<u>Marketplace AWS</u> <u>aggiornamento del sito Web a IPv6 entro dicembre 2022</u>	Si consiglia agli acquirenti che attualmente utilizzano l'indirizzo in formato IPv4 nelle proprie politiche IAM di aggiornare le proprie politiche IAM agli indirizzi in formato IPv6 prima del 15 dicembre 2022.	29 settembre 2022
<u>Marketplace AWS</u> <u>Autorizzazioni granulari per il marketplace privato</u>	Gli acquirenti ora dispongono di autorizzazioni più dettagliate per gestire le esperienze di marketplace private.	8 settembre 2022
<u>Sono state aggiunte due politiche per Marketplace AWS</u> <u>Vendor Insights.</u>	Sono state aggiunte due politiche AWSVendor InsightsAssessorFullAccess e, AWSVendor InsightsAssessorReadOnly per Marketplace AWS Vendor Insights, una funzionalità che offre la valutazione del rischio del software	26 luglio 2022
<u>Informazioni dettagliate sui fornitori Marketplace AWS</u>	Marketplace AWSVendor Insights è una funzionalità che offre la valutazione del rischio del software.	26 luglio 2022
<u>Aggiornamento dei metodi di pagamento</u>	Aggiornamento della sola documentazione per chiarire come modificare i metodi di pagamento nella console di fatturazione. AWS	1 giugno 2022

<u>Prove gratuite SaaS per contratti</u>	Gli acquirenti possono ora abbonarsi alle prove gratuite SaaS per contratti per esplorare i prodotti prima di passare alle versioni di prova a pagamento.	31 maggio 2022
<u>Aggiunti tag di misurazione del fornitore per prodotti AMI, Container e SaaS</u>	Nuova funzionalità che fornisce tag per aiutare i clienti a comprendere l'utilizzo Marketplace AWS delle risorse in base alle metriche fornite dal fornitore.	27 maggio 2022
<u>Notifiche e-mail aggiunte alle transazioni degli acquirenti</u>	Nuova funzionalità che consente di inviare notifiche e-mail all'acquirente per verificare gli accordi stipulati. Marketplace AWS	23 maggio 2022
<u>È stata abilitata l'approvazione automatica dei prodotti Free/ByoL per i clienti di eProcurement</u>	I clienti possono utilizzare immediatamente i prodotti con la nuova approvazione automatica dei prodotti Free/ByoL per i clienti di eProcurement.	2 maggio 2022
<u>Modifiche contrattuali abilitate per gli acquirenti nei contratti AMI e Container Product</u>	I contratti sui prodotti AMI e Container possono essere modificati per acquistare diritti aggiuntivi o abilitare l'opzione di rinnovo automatico dell'abbonamento.	6 aprile 2022

<u>Capacità di tenere traccia dell'utilizzo della licenza</u>	Gli acquirenti possono ora tenere traccia delle metriche di licenza basate sull'utilizzo per i prodotti AMI e SaaS con. AWS License Manager	28 marzo 2022
<u>Aggiornamenti alla versione Helm CLI</u>	Documentazione aggiornata dei prodotti container relativa alla modifica della versione Helm CLI da 3.7.0 a 3.7.1. Questa è l'unica versione compatibile al momento.	8 marzo 2022
<u>Aggiornamenti alle politiche gestite esistenti</u>	Le autorizzazioni che non erano più necessarie sono state rimosse dalle seguenti politiche: AWSMarketplaceFullAccess eAWSMarketplaceImageBuildFullAccess .	4 marzo 2022
<u>Possibilità per gli acquirenti con sede nell'area EMEA di acquistare prodotti tramite Amazon Web Services EMEA SARL</u>	Marketplace AWSGli acquirenti con sede in paesi e territori in Europa, Medio Oriente e Africa (EMEA), esclusi Turchia e Sud Africa, possono ora ricevere Marketplace AWS fatture tramite Amazon Web Services EMEA SARL per gli acquisti da venditori idonei all'area EMEA. Account AWS	7 gennaio 2022
<u>Supporto per la regione Asia Pacifico (Giacarta)</u>	Marketplace AWSora supporta quanto segueRegione AWS: Asia Pacifico (Giacarta).	13 dicembre 2021

[Metodo di consegna Helm chart per prodotti basati su container](#)

Gli acquirenti possono ora lanciare prodotti basati su container installando un grafico Helm nei loro ambienti di lancio.

29 novembre 2021

[Aggiornamenti generali e riorganizzazione della documentazione dei prodotti basati su container](#)

Documentazione aggiornata sui prodotti basati su container per aggiungere maggiori informazioni e chiarezza sulla ricerca, la sottoscrizione e il lancio di prodotti basati su container.

29 novembre 2021

[Documentazione aggiunta per QuickLaunch](#)

Gli acquirenti possono ora QuickLaunch utilizzarlo per lanciare prodotti basati su container con un metodo di consegna Helm chart. QuickLaunch è una funzionalità Marketplace AWS che sfrutta la creazione rapida AWS CloudFormation di un nuovo cluster Amazon EKS e il lancio di un'applicazione basata su di esso.

29 novembre 2021

[Prezzi contrattuali per prodotti basati su AMI e prodotti basati su container](#)

Gli acquirenti possono ora acquistare un prodotto basato su AMI o un prodotto basato su container con prezzi anticipati.

17 novembre 2021

Support per gli ordini di acquisto nei prodotti SaaS	Marketplace AWSsupporta l'aggiunta di numeri d'ordine di acquisto agli acquisti di contratti Software as a Service (SaaS).	28 ottobre 2021
Support per l'integrazione con SAP Ariba	Marketplace AWSsupporta l'integrazione con il sistema di approvvigionamento SAP Ariba.	13 ottobre 2021
Support per alias AMI	Marketplace AWSsupporta l'utilizzo di alias per gli ID AMI che possono essere utilizzati in tutte le regioni.	8 settembre 2021
Sono state rimosse le autorizzazioni non utilizzate nella politica gestita	Le autorizzazioni non utilizzate e dalla politica <code>AWSPrivat eMarketplaceAdminF ullAccess</code> AWS gestita sono state rimosse.	27 agosto 2021
Support per la condivisione delle licenze tramite AWS License Manager	Puoi condividere le licenze dei prodotti acquistati con altri account della tua AWS organizzazione.	3 dicembre 2020
Marketplace AWSsupporta l'offerta di servizi professionali	Marketplace AWSora supporta l'acquisto di servizi professionali.	3 dicembre 2020
Support per la valuta preferita	Puoi pagare gli Marketplace AWS acquisti utilizzando la tua valuta preferita.	27 luglio 2020

Puoi esaminare e accettare offerte private, upgrade e rinnovi.	I venditori possono fornire offerte private di aggiornamento e rinnovo per il contratto SaaS e il contratto SaaS con prodotti di consumo che puoi esaminare e accettare durante un contratto esistente.	28 maggio 2020
Marketplace AWS supporta prodotti di dati tramite AWS Data Exchange	Ora puoi abbonarti ai prodotti di dati AWS Data Exchange in Marketplace AWS.	13 novembre 2019
Marketplace AWS supporta container con cadenza oraria a pagamento	Marketplace AWS ora supporta container orari a pagamento in esecuzione su Amazon Elastic Kubernetes Service (Amazon EKS).	25 settembre 2019
Offerte private aggiornate su Marketplace AWS	Contenuti aggiornati per fornire maggiori informazioni sull'accettazione di diversi tipi di offerte private.	29 marzo 2019
Sicurezza aggiornata su Marketplace AWS	Informazioni aggiornate sulle policy IAM, sezione ristrutturata per la leggibilità.	25 marzo 2019
Contenuto aggiunto per la funzionalità di marketplace privato	Aggiunti contenuti a supporto del rilascio di Private Marketplace.	27 novembre 2018
Versione iniziale della guida per l'utente per gli acquirenti	Versione iniziale della Guida Marketplace AWS all'acquisto.	16 novembre 2018

AWS Glossario

Per la AWS terminologia più recente, consultate il [AWS glossario](#) nella sezione Reference. Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.