Guida per l'utente

AWS Artifact

AWS Artifact: Guida per l'utente

Table of Contents

Cos'è AWS Artifact? 1
Prezzi 1
Nozioni di base 2
Fase 1: Registrazione ad AWS 2
Fase 2: Scaricare un rapporto 3
Fase 3: Gestire gli accordi 3
Fase 4: Gestire le notifiche 4
Scaricamento dei report 6
Scaricamento di un rapporto 6
Visualizzazione degli allegati nei documenti PDF 7
Proteggi i tuoi documenti 7
Risoluzione dei problemi 8
Gestione degli accordi 9
Accordi per un singolo account 9
Accettazione di un accordo con AWS 9
Risoluzione di un contratto con AWS 10
Accordi per più account 11
Accettazione di un contratto per la tua organizzazione 11
Risoluzione di un accordo organizzativo 12
Accordi offline 13
Gestione delle notifiche 15
Configurazione delle notifiche 15
Assegnazione di tag a una configurazione 17
Risoluzione dei problemi 17
Gestione dell'identità e degli accessi 18
Configura l'accesso utente a AWS Artifact 18
Fase 1: Creazione di una policy IAM 19
Fase 2: Creare un gruppo IAM e allegare la policy 19
Passaggio 3: crea utenti IAM e aggiungili al gruppo 20
Migrazione verso autorizzazioni granulari 20
Migrazione a nuove autorizzazioni 21
Policy IAM di esempio 23
Utilizzo delle policy gestite in AWS 36
AWSArtifactReportsReadOnlyAccess 37

Aggiornamenti alle policy 37
Uso di ruoli collegati ai servizi 38
Autorizzazioni di ruolo collegate ai servizi per AWS Artifact 38
Creazione di un ruolo collegato ai servizi per AWS Artifact 39
Modifica di un ruolo collegato ai servizi per AWS Artifact 39
Eliminazione di un ruolo collegato al servizio per AWS Artifact 39
Regioni supportate per i ruoli collegati ai servizi AWS Artifact 40
Utilizzo delle chiavi di condizione IAM 41
CloudTrail disboscamento 45
..... 45
AWS Artifactinformazioni in CloudTrail 45
Comprensione delle voci dei file di log di AWS Artifact 46
Cronologia dei documenti 49
..... lii

Cos'è AWS Artifact?

AWS Artifactfornisce download su richiesta di documenti diAWS sicurezza e conformità, come certificazioniAWS ISO, report PCI (Payment Card Industry) e report SOC (Service Organization Control). Puoi inoltrare i documenti sulla sicurezza e la conformità (anche noti come artefatti di audit) a revisori e autorità di regolamentazione per dimostrare la sicurezza e la conformità delle infrastrutture e dei servizi AWS che utilizzi Puoi anche utilizzare questi documenti come linee guida per valutare la tua architettura cloud e valutare l'efficacia dei controlli interni della tua azienda.

Inoltre,AWS Artifact fornisce download su richiesta dei documenti di sicurezza e conformità, come le certificazioni ISO e i report SOC (Service Organization Control) dei fornitori di software indipendenti (ISV) che vendono i propri prodotti suMarketplace AWS. Per ulteriori informazioni, consulta la pagina relativa ai Marketplace AWSVendor Insights.

AWSi clienti sono responsabili dello sviluppo o dell'ottenimento di documenti che dimostrino la sicurezza e la conformità delle loro aziende. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

Puoi anche usare AWS Artifact per riesaminare, accettare e tracciare lo stato degli accordi AWS come il Business Associate Addendum (BAA). Generalmente un accordo BAA viene richiesto alle aziende che sono soggette all'Health Insurance Portability and Accountability Act (HIPAA) per garantire che i dati sanitari protetti (PHI) siano salvaguardati in modo adeguato. Con AWS Artifact, puoi accettare accordi con AWS e designare account AWS che possano elaborare giuridicamente informazioni limitate. Puoi accettare un accordo per conto di più account. Per accettare gli accordi per più account, usa AWS Organizations per creare un'organizzazione.

Per ulteriori informazioni, consulta AWS Artifact.

Prezzi

AWSti fornisceAWS Artifact documenti e accordi gratuitamente.

Nozioni di base su AWS Artifact

AWS Artifactfornisce una risorsa centrale per i report AWS di sicurezza e conformità. Gli elementi disponibili AWS Artifact includono i report SOC (Service Organization Control), i report PCI (Payment Card Industry) e le certificazioni degli organismi di accreditamento che convalidano l'implementazione e l'efficacia operativa dei controlli di sicurezza. AWS Inoltre, AWS Artifact fornisce l'accesso su richiesta ai documenti di sicurezza e conformità, come le certificazioni ISO e i report SOC (Service Organization Control) degli Independent Software Vendors (ISV) su cui vendono i propri prodotti. Marketplace AWS Per ulteriori informazioni, consulta Vendor Insights. Marketplace AWS

AWS Artifactconsente di accettare e gestire accordi legali come il Business Associate Addendum (BAA). Se usi AWS Organizations, puoi accettare accordi per conto di tutti gli account all'interno della tua organizzazione. Una volta accettati, tutti gli account membro esistenti e futuri sono automaticamente coperti dall'accordo.

Attività

- Fase 1: Registrazione ad AWS
- Fase 2: Scaricare un rapporto
- Fase 3: Gestire gli accordi
- Fase 4: Gestire le notifiche

Fase 1: Registrazione ad AWS

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Per registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Fase 2: Scaricare un rapporto

Puoi scaricare i report utilizzando Adobe Acrobat Reader. Gli altri lettori PDF non sono supportati. Per ulteriori informazioni, consulta Scaricamento dei report.

Per scaricare un report

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nella AWS Artifact home page, scegli Visualizza report.
3. Nella pagina Report, utilizza la scheda AWSreport per accedere a un AWS report e vai alla scheda Report di terze parti per accedere ai report degli Independent Software Vendors (ISV) su cui vendono i loro prodotti. Marketplace AWS
4. (Facoltativo) Inserisci una parola chiave nel campo di ricerca per individuare un rapporto.
5. Seleziona un rapporto, quindi scegli Scarica rapporto.
6. (Facoltativo) Nella scheda Rapporti di terze parti, puoi accedere alla pagina dei dettagli di un rapporto ISV facendo clic sul titolo del rapporto per ulteriori informazioni sul rapporto.
7. È possibile che ti venga chiesto di accettare i termini e le condizioni applicabili al rapporto specifico che stai scaricando. Ti consigliamo di leggerli attentamente. Al termine, seleziona Ho letto e accetto i termini, quindi scegli Accetta i termini e scarica il rapporto.
8. Apri il file scaricato tramite un visualizzatore di PDF. Consulta i termini e le condizioni per l'accettazione e scorri verso il basso per trovare il rapporto di audit. I report potrebbero contenere informazioni aggiuntive incorporate come allegati all'interno del documento PDF, quindi assicurati di verificare la presenza di allegati nel file PDF per la documentazione di supporto. Consulta questa pagina per istruzioni su come visualizzare gli allegati.

I report di terze parti sono accessibili solo per AWS i clienti che hanno effettuato l'accesso a Marketplace AWS Vendor Insights. Per ulteriori informazioni, consulta Marketplace AWS Vendor Insights.

Fase 3: Gestire gli accordi

Prima di stipulare un contratto, è necessario scaricare e accettare i termini dell'accordo di AWS Artifact non divulgazione (NDA). Ogni accordo è riservato e non può essere condiviso con altre persone esterne all'azienda.

Per accettare un accordo con AWS

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel riquadro di navigazione di AWS Artifact, scegliere Agreements (Accordi).
3. Scegli Account agreement per gestire gli accordi per il tuo account o Account agreement per gestire gli accordi per conto della tua organizzazione.
4. Espandi la sezione del contratto.
5. Scegli Scarica e rivedi.
6. Leggi i termini e le condizioni. Quando hai finito, scegli Accetta e scarica.
7. Controlla l'accordo, quindi seleziona le caselle di controllo per indicare che sei d'accordo.
8. Scegli Accetta per accettare l'accordo.

Per ulteriori informazioni, consulta Gestione degli accordi.

Fase 4: Gestire le notifiche

Puoi iscriverti alle notifiche relative alla disponibilità di nuovi report e accordi o agli aggiornamenti di report e accordi esistenti. AWS Artifact utilizza il servizio AWS User Notification per inviare notifiche. Le notifiche vengono inviate agli indirizzi e-mail forniti dall'utente durante la configurazione della configurazione delle notifiche.

Per creare una configurazione

1. Apri la pagina degli hub di notifica nel servizio AWS User Notifications
2. Seleziona le regioni in cui desideri archiviare le risorse AWS User Notifications. Per impostazione predefinita, i dati delle notifiche utente verranno archiviati negli Stati Uniti orientali (Virginia settentrionale) e replicati in altre regioni selezionate. Per maggiori dettagli, consulta la documentazione degli hub di notifica.
3. Fai clic su Crea configurazione.
4. Per ricevere notifiche relative agli accordi, fai clic sulla casella di controllo Updates on AWS Agreements.
5. Per ricevere notifiche relative ai report, fai clic sulla casella di controllo Updates on AWS Reports. Per ricevere notifiche solo per i report in categorie e serie specifiche, fai clic sulla casella di controllo relativa a Un sottoinsieme di report e fai clic sulla casella di controllo per le categorie e le serie che ti interessano.

6. Inserisci un nome per la tua configurazione.
7. Inserisci un elenco di e-mail separate da virgole a cui inviare le notifiche.
8. (Facoltativo) Per assegnare un tag alla configurazione della notifica, inserisci le coppie chiave-valore espandendo la sezione Tag. Nota: un tag è un'etichetta che puoi assegnare a una risorsa AWS e ogni tag è costituito da una chiave e da un valore opzionale che puoi definire. I tag ti aiutano a gestire, cercare e filtrare le risorse.
9. Fare clic su Submit (Invia).
10. Verrà inviata un'e-mail di verifica agli indirizzi e-mail forniti e i destinatari dell'e-mail dovranno fare clic sul collegamento Verifica e-mail all'interno dell'e-mail di verifica inviata loro. Tieni presente che solo gli indirizzi e-mail verificati inizieranno a ricevere notifiche.

Per ulteriori informazioni, consulta Gestione delle notifiche.

Scaricamento dei report in AWS Artifact

Puoi eseguire il download dei rapporti dalla console AWS Artifact. Quando scarichi un rapporto da AWS Artifact, quest'ultimo viene generato specificamente per te e ogni rapporto ha una filigrana univoca. Per questo motivo, è consigliabile condividere i rapporti solo con chi reputi attendibile. Non inviare i rapporti come allegati delle email e non condividerli online. Per condividere un report, utilizza un servizio di condivisione sicuro come Amazon WorkDocs. Alcuni report richiedono l'accettazione dei Termini e condizioni prima di poterli scaricare.

Indice

- Scaricamento di un rapporto
- Visualizzazione degli allegati nei documenti PDF
- Proteggi i tuoi documenti
- Risoluzione dei problemi

Scaricamento di un rapporto

Per scaricare un rapporto, è necessario disporre delle autorizzazioni necessarie. Per ulteriori informazioni, consulta Identity and Access Management in AWS Artifact.

Quando ti registri a AWS Artifact, il tuo account ottiene automaticamente l'autorizzazione per scaricare alcuni rapporti. In caso di problemi di accessoAWS Artifact, segui le istruzioni nella pagina di riferimento sull'autorizzazione del AWS Artifact servizio.

Per scaricare un report

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nella AWS Artifact home page, scegli Visualizza report.
3. Nella pagina Report, utilizza la scheda AWSreport per accedere a un AWS report e vai alla scheda Report di terze parti per accedere ai report degli Independent Software Vendors (ISV) su cui vendono i loro prodotti. Marketplace AWS
4. (Facoltativo) Inserisci una parola chiave nel campo di ricerca per individuare un rapporto.
5. Seleziona un rapporto, quindi scegli Scarica rapporto.
6. (Facoltativo) Nella scheda Rapporti di terze parti, puoi accedere alla pagina dei dettagli di un rapporto ISV facendo clic sul titolo del rapporto per ulteriori informazioni sul rapporto.

7. È possibile che ti venga chiesto di accettare i termini e le condizioni applicabili al rapporto specifico che stai scaricando. Ti consigliamo di leggerli attentamente. Al termine, seleziona Ho letto e accetto i termini, quindi scegli Accetta i termini e scarica il rapporto.
8. Apri il file scaricato tramite un visualizzatore di PDF. Consulta i termini e le condizioni per l'accettazione e scorri verso il basso per trovare il rapporto di audit. I report potrebbero contenere informazioni aggiuntive incorporate come allegati all'interno del documento PDF, quindi assicurati di verificare la presenza di allegati nel file PDF per la documentazione di supporto. Consulta questa pagina per istruzioni su come visualizzare gli allegati.

Visualizzazione degli allegati nei documenti PDF

Si consigliano le seguenti applicazioni che attualmente supportano la visualizzazione degli allegati PDF:

Adobe Acrobat Viewer

1. Scarica l'ultima versione di Adobe Acrobat da qui.
2. Apri il file nel visualizzatore Adobe Acrobat.
3. Per aprire il pannello Allegati, fate clic sull'icona a forma di graffetta a sinistra del documento PDF o scegliete Visualizza > Mostra/Nascondi > Pannelli di navigazione > Allegati.
4. Nel pannello Allegati, fate doppio clic sull'allegato per visualizzare il documento.

Browser Firefox

1. Scarica il browser Firefox da qui
2. Apri il file PDF nel browser Firefox utilizzando l'opzione Apri file dal menu File.
3. Per aprire gli allegati, fai clic sull'icona Toggle nella barra laterale in alto a sinistra dello schermo.

Proteggi i tuoi documenti

AWS Artifacti documenti sono riservati e devono essere tenuti al sicuro in ogni momento. AWS Artifactutilizza il modello di responsabilità AWS condivisa per i propri documenti. Ciò significa che AWS è responsabile della protezione dei documenti mentre sono nel AWS Cloud, ma l'utente è responsabile della loro protezione dopo averli scaricati. AWS Artifactpotrebbe richiederti di accettare

i Termini e condizioni prima di poter scaricare i documenti. Ogni download dei documenti ha una filigrana univoca e tracciabile.

È consentito condividere documenti contrassegnati come riservati solo all'interno della propria azienda, con le autorità di regolamentazione e con i revisori. Non è consentito condividere questi documenti con i tuoi clienti o sul tuo sito Web. Ti consigliamo vivamente di utilizzare un servizio di condivisione di documenti sicuro, come Amazon WorkDocs, per condividere documenti con altri. Non inviare i documenti tramite e-mail o caricarli su un sito non sicuro.

Risoluzione dei problemi

Se non riesci a scaricare un documento o ricevi un messaggio di errore, consulta Risoluzione dei problemi nelle AWS Artifact Domande frequenti.

Gestione degli accordi in AWS Artifact

AWS Artifact Agreements ti consente di utilizzare la AWS Management Console per riesaminare, accettare e gestire gli accordi del tuo account o della tua organizzazione. Ad esempio, un accordo Business Associate Addendum (BAA) generalmente viene richiesto per le aziende soggette all'Health Insurance Portability and Accountability Act (HIPAA) per garantire che i dati sanitari protetti (PHI) siano salvaguardati in modo adeguato. Per accettare un accordo come il BAA, puoi utilizzare AWS Artifact con AWS e indicare un account AWS che possa elaborare giuridicamente i dati sanitari protetti. Se usi AWS Organizations puoi accettare accordi come il AWS BAA per conto di tutti gli account della tua organizzazione. Tutti gli account membro esistenti e successivi sono automaticamente coperti dall'accordo e possono elaborare giuridicamente i dati sanitari protetti.

Puoi usare AWS Artifact anche per confermare che il tuo account o la tua organizzazione AWS accetti l'accordo, per esaminare i termini dell'accordo accettato e conoscerne gli obblighi. Se il tuo account o la tua organizzazione non devono più utilizzare il contratto accettato, puoi utilizzare AWS Artifact per risolvere il contratto. Se risolvi il contratto ma in seguito ti rendi conto che ne hai bisogno, puoi riattivarlo.

Indice

- Gestione di un contratto per un singolo account in AWS Artifact
- Gestione di un contratto per più account in AWS Artifact
- Gestione di un accordo offline esistente in AWS Artifact

Gestione di un contratto per un singolo account in AWS Artifact

Puoi accettare gli accordi solo per il tuo account, anche se il tuo è un account membro di un'organizzazione in AWS Organizations. Per ulteriori informazioni su AWS Organizations, consulta la Guida per l'utente di AWS Organizations.

Accettazione di un accordo con AWS

Prima di accettare un accordo, ti consigliamo di contattare il tuo team di legali, della privacy e di conformità.

Autorizzazioni richieste

Se sei l'amministratore di un account, puoi concedere agli utenti IAM e agli utenti federati con ruoli le autorizzazioni per accedere e gestire uno o più dei tuoi accordi. Per impostazione predefinita, solo gli utenti con privilegi di amministratore possono accettare un accordo. Per accettare un accordo, IAM e gli utenti federati devono disporre delle seguenti autorizzazioni:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Per accettare un accordo con AWS

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel riquadro di navigazione di AWS Artifact, scegliere Agreements (Accordi).
3. Selezionare la scheda Accordi account.
4. Espandi la sezione del contratto.
5. Scegli Scarica e rivedi.
6. Leggi i Termini e condizioni. Quando hai finito, scegli Accetta e scarica.
7. Controlla l'accordo, quindi seleziona le caselle di controllo per indicare che sei d'accordo.
8. Scegli Accetta per accettare l'accordo per il tuo account.

Risoluzione di un contratto con AWS

Se hai utilizzato la console AWS Artifact per accettare un accordo, puoi usare la console per cessare quell'accordo. In caso contrario, consulta Accordi offline.

Autorizzazioni richieste

Per recedere da un contratto, IAM e gli utenti federati devono disporre delle seguenti autorizzazioni:

```
artifact:TerminateAgreement
```

Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Per cessare il tuo accordo online con AWS

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel riquadro di navigazione di AWS Artifact, scegliere Agreements (Accordi).

3. Selezionare la scheda Accordi account.
4. Seleziona il contratto e scegli Termina contratto.
5. Seleziona tutte le caselle di controllo per indicare che accetti di recedere dal contratto.
6. Scegliere Terminate (Termina). Quando viene richiesta la conferma, seleziona Terminate (Termina).

Gestione di un contratto per più account in AWS Artifact

Se sei il proprietario dell'account di gestione di un'AWS Organizationsorganizzazione, puoi accettare un accordo per conto di tutti gli account dell'organizzazione. È necessario accedere all'account di gestione con le AWS Artifact autorizzazioni corrette per accettare o recedere dai contratti organizzativi. Gli utenti degli account membri con autorizzazioni `organizations:DescribeOrganization`, possono visualizzare gli accordi dell'organizzazione accettati per conto loro.

Se il tuo account non fa parte di un'organizzazione, puoi creare o entrare a far parte di un'organizzazione seguendo le istruzioni in Creare e gestire un'organizzazione nella Guida per l'AWS Organizationsutente.

AWS Organizations offre due set di funzioni: fatturazione consolidata e tutte le caratteristiche. Per usare AWS Artifact per la tua organizzazione, quest'ultima deve essere abilitata a tutte le caratteristiche. Se la tua organizzazione è configurata solo per la fatturazione consolidata, consulta Abilitazione di tutte le funzionalità dell'organizzazione nella Guida per l'AWS Organizationsutente.

Se un account membro viene rimosso da un'organizzazione, non sarà più coperto dagli accordi dell'organizzazione. Prima della rimozione, gli amministratori degli account di gestione devono avvertire gli account membri che saranno rimossi dall'organizzazione, per consentire loro di attivare nuovi accordi se necessario. Un elenco degli accordi organizzativi attivi può essere visualizzato in Accordi AWS Artifactorganizzativi.

Per ulteriori informazioni, consulta Managing the AWS accounts in your organization nella AWS OrganizationsUser Guide.

Accettazione di un contratto per la tua organizzazione

Puoi accettare un accordo per conto di tutti gli account membri della tua organizzazione in AWS Organizations. Prima di accettare un accordo, ti consigliamo di contattare il tuo team di legali, della privacy e di conformità.

Autorizzazioni richieste

Per accettare un accordo, il proprietario dell'account di gestione deve disporre delle seguenti autorizzazioni:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Per accettare un accordo per un'organizzazione

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel pannello di controllo AWS Artifact, scegliere Agreements (Accordi).
3. Scegliere la scheda Accordi organizzazione.
4. Espandi la sezione del contratto.
5. Scegli Scarica e rivedi.
6. Leggi i Termini e condizioni. Quando hai finito, scegli Accetta e scarica.
7. Controlla l'accordo, quindi seleziona le caselle di controllo per indicare che sei d'accordo.
8. Scegliere Accetta per accettare l'accordo per tutti gli account esistenti e futuri della tua organizzazione.

Risoluzione di un accordo organizzativo

Se hai usato la console AWS Artifact per accettare un accordo per conto di tutti gli account membri di un'organizzazione, puoi usare la console per cessare quell'accordo. In caso contrario, consulta Accordi offline.

Autorizzazioni richieste

Per recedere da un contratto, il proprietario dell'account di gestione deve disporre delle seguenti autorizzazioni:

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Per cessare l'accordo online della tua organizzazione con AWS

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel pannello di controllo AWS Artifact, scegliere Agreements (Accordi).
3. Scegliere la scheda Accordi organizzazione.
4. Seleziona il contratto e scegli Termina contratto.
5. Seleziona tutte le caselle di controllo per indicare che accetti di recedere dal contratto.
6. Scegliere Terminate (Termina). Quando viene richiesta la conferma, seleziona Terminate (Termina).

Gestione di un accordo offline esistente in AWS Artifact

Se hai già un accordo offline, AWS Artifact visualizza gli accordi che hai accettato offline. Ad esempio, la console potrebbe visualizzare l'accordo Offline Business Associate Addendum (BAA) con lo stato Attivo. Lo stato attivo indica che l'accordo è stato accettato. Per cessare un accordo offline, consulta le linee guida sulla cessazione e le istruzioni incluse nel tuo accordo.

Se il tuo account è l'account di gestione di un'AWS Organizationsorganizzazione, puoi AWS Artifact utilizzarlo per applicare i termini del contratto offline a tutti gli account dell'organizzazione. Per applicare alla tua organizzazione e a tutti gli account presenti nella tua organizzazione un accordo che hai accettato offline, devi disporre delle autorizzazioni seguenti:

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Se il tuo è un account membro all'interno di un'organizzazione, per visualizzare gli accordi offline dell'organizzazione devi disporre delle autorizzazioni seguenti:

```
organizations:DescribeOrganization
```

Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Gestione delle notifiche in AWS Artifact

Le notifiche di AWS Artifact ti consentono di configurare notifiche e-mail. Nella pagina delle impostazioni di notifica, puoi iscriverti alle notifiche e gestire altre impostazioni di notifica come descritto di seguito. AWS Artifact invia notifiche utilizzando il servizio AWS User Notifications. Per utilizzare le notifiche AWS Artifact devi disporre delle autorizzazioni necessarie per i servizi AWS Artifact e AWS User Notification. Per ulteriori informazioni, consulta Gestione dell'identità e degli accessi.

Indice

- Configurazione delle notifiche
- Assegnazione di tag a una configurazione
- Risoluzione dei problemi

Configurazione delle notifiche

Prima di iniziare a ricevere notifiche, dovrai specificare le regioni in cui verranno archiviati i dati delle notifiche utente. Segui i passaggi seguenti per configurare gli hub di notifica.

Per configurare gli hub di notifica

1. Apri la pagina degli hub di notifica nel servizio AWS User Notifications.
2. Seleziona le regioni in cui desideri archiviare le risorse AWS User Notifications. Per impostazione predefinita, i dati delle notifiche utente verranno archiviati negli Stati Uniti orientali (Virginia settentrionale) e replicati nelle altre regioni selezionate. Per ulteriori dettagli, consulta la documentazione degli hub di notifica.
3. Fare clic su Submit (Invia).

Per iscriversi alle notifiche di

1. Apri la pagina delle impostazioni di notifica di AWS Artifact.
2. Fai clic sull'interruttore Iscriviti alle notifiche di Artifact per iscriverti alle notifiche su AWS Artifact.

Per annullare l'iscrizione alle notifiche

1. Apri la pagina delle impostazioni di notifica di AWS Artifact.
2. Fai clic sull'interruttore Iscriviti alle notifiche di Artifact per annullare l'iscrizione alle notifiche su AWS Artifact.

Per creare una configurazione

1. Apri la pagina delle impostazioni di notifica di AWS Artifact.
2. Fai clic su Crea configurazione.
3. Per ricevere notifiche relative agli accordi, tieni selezionata la casella di controllo accanto a Updates on AWS Agreements.
4. Per ricevere notifiche per i report, tieni selezionata la casella di controllo accanto a Updates on AWS Reports.
5. Per ricevere notifiche per tutti i report, tieni selezionata la casella di controllo accanto a Tutti i report.
6. Per ricevere notifiche solo per i report rientranti in categorie e serie specifiche, fai clic sulla casella di controllo Un sottoinsieme di report. Quindi, fai clic sulla casella di controllo relativa alle categorie e alle serie che ti interessano.
7. Inserisci un nome per la tua configurazione.
8. Inserisci un elenco di e-mail separate da virgole a cui inviare le notifiche.
9. (Facoltativo) Per assegnare un tag alla configurazione delle notifiche, inserisci le coppie chiave-valore espandendo la sezione Tag. Nota: un tag è un'etichetta che puoi assegnare a una risorsa AWS e ogni tag è costituito da una chiave e da un valore opzionale che puoi definire. I tag ti aiutano a gestire, cercare e filtrare le risorse.
10. Fai clic su Crea configurazione.
11. Verrà inviata un'e-mail di verifica agli indirizzi e-mail forniti e i destinatari dell'e-mail dovranno fare clic sul collegamento Verifica e-mail all'interno dell'e-mail di verifica inviata loro. Tieni presente che solo gli indirizzi e-mail verificati inizieranno a ricevere notifiche.

Per modificare una configurazione

1. Apri la pagina delle impostazioni di notifica di AWS Artifact.
2. Fai clic sulla riga della configurazione che desideri modificare.

3. Fai clic sul pulsante Modifica in alto a destra della pagina.
4. Puoi modificare qualsiasi campo. Quando sei soddisfatto della modifica, premi Salva modifiche.
5. Se hai aggiunto nuovi indirizzi e-mail, verrà inviata un'email di verifica a ciascuno di questi indirizzi e-mail. Fai clic sul link Verifica e-mail all'interno dell'e-mail di verifica.

Per eliminare una configurazione

1. Apri la pagina delle impostazioni di notifica di AWS Artifact.
2. Fai clic sulla riga della configurazione che desideri eliminare.
3. Fai clic su Delete (Elimina).
4. Dopo aver letto il messaggio di avviso, fai clic su Elimina.

Assegnazione di tag a una configurazione

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag consentono di gestire, cercare e filtrare le risorse. Facoltativamente, puoi impostare i tag quando crei o modifichi una configurazione. Per saperne di più, consulta Taggare le risorse

Risoluzione dei problemi

Se ricevi un messaggio di errore durante l'utilizzo delle notifiche di AWS Artifact, consulta Risoluzione dei problemi nelle Domande frequenti. AWS Artifact

Identity and Access Management in AWS Artifact

Quando ti registri a AWS, fornisci un indirizzo email e una password che sono associati al tuo nuovo account AWS. Queste sono le tue credenziali root e forniscono l'accesso completo a tutte le tue AWS risorse, incluse le risorse perAWS Artifact. Tuttavia, consigliamo fortemente di non usare l'account root per gli accessi quotidiani. Consigliamo anche di non condividere le credenziali dell'account con altri, permettendo loro l'accesso completo al tuo account.

Invece di accedere al tuo AWS account con credenziali root o condividere le tue credenziali con altri, dovresti creare un'identità utente speciale chiamata utente IAM per te e per chiunque abbia bisogno di accedere a un documento o a un accordo in. AWS Artifact Così facendo, puoi fornire informazioni di accesso individuali per ogni utente e puoi concedere a ogni utente solo le autorizzazioni di cui hanno bisogno per lavorare con documenti specifici. Puoi anche concedere a più utenti IAM le stesse autorizzazioni concedendo le autorizzazioni a un gruppo IAM e aggiungendo gli utenti IAM al gruppo.

Se gestisci già le identità degli utenti all'esternoAWS, puoi utilizzare i provider di identità IAM invece di creare utenti IAM. Per ulteriori informazioni, consulta Provider di identità e federazione nella Guida per l'utente IAM.

Indice

- Configura l'accesso utente a AWS Artifact
- Migrazione verso autorizzazioni granulari
- Policy IAM di esempio
- AWSpolitiche gestite per AWS Artifact
- Utilizzo di ruoli collegati ai servizi per AWS Artifact
- Utilizzo delle chiavi di condizione IAM

Configura l'accesso utente a AWS Artifact

Completa i seguenti passaggi per concedere agli utenti le autorizzazioni AWS Artifact in base al livello di accesso di cui hanno bisogno.

Attività

- Fase 1: Creazione di una policy IAM

- Fase 2: Creare un gruppo IAM e allegare la policy
- Passaggio 3: crea utenti IAM e aggiungili al gruppo

Fase 1: Creazione di una policy IAM

In qualità di amministratore IAM, puoi creare una policy che conceda AWS Artifact autorizzazioni ad azioni e risorse.

Per creare una policy IAM

Utilizza la seguente procedura per creare una policy IAM da utilizzare per concedere le autorizzazioni agli utenti e ai gruppi IAM.

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Scegliere la scheda JSON.
5. Inserisci un documento di policy. È possibile creare la propria politica oppure utilizzare una delle politiche diPolicy IAM di esempio.
6. Scegliere Review policy (Esamina policy). In Validatore di policy vengono segnalati eventuali errori di sintassi.
7. Nella pagina Rivedi la politica, inserisci un nome univoco che ti aiuti a ricordare lo scopo della politica. Puoi anche fornire una descrizione.
8. Scegli Crea policy.

Fase 2: Creare un gruppo IAM e allegare la policy

In qualità di amministratore IAM, puoi creare un gruppo e allegare la policy che hai creato al gruppo. Puoi aggiungere utenti IAM al gruppo in qualsiasi momento.

Per creare un gruppo IAM e allegare la tua policy

1. Nel riquadro di navigazione scegliere Groups (Gruppi), quindi Create New Group (Crea nuovo gruppo).
2. Per Nome gruppo, inserisci un nome per il tuo gruppo, quindi scegli Passaggio successivo.

3. Nel campo di ricerca, inserisci il nome della politica che hai creato. Seleziona la casella di controllo relativa alla tua politica, quindi scegli Passaggio successivo.
4. Verifica il nome e le policy del gruppo. Quando sei pronto, scegli Crea gruppo.

Passaggio 3: crea utenti IAM e aggiungili al gruppo

In qualità di amministratore IAM, puoi aggiungere utenti a un gruppo in qualsiasi momento. Ciò concede agli utenti le autorizzazioni concesse al gruppo.

Per creare un utente IAM e aggiungerlo a un gruppo

1. Nel pannello di navigazione seleziona Utenti, quindi Aggiungi utente.
2. Per Nome utente, inserisci i nomi di uno o più utenti.
3. Seleziona la casella di controllo accanto ad Accesso alla AWS Management Console. Configura una password generata automaticamente o personalizzata. Facoltativamente, puoi selezionare L'utente deve creare una nuova password al prossimo accesso per richiedere la reimpostazione della password al primo accesso dell'utente.
4. Scegli Successivo: Autorizzazioni.
5. Scegli Aggiungi utente al gruppo, quindi seleziona il gruppo che hai creato.
6. Scegliere Successivo: Tag. Facoltativamente, puoi aggiungere tag ai tuoi utenti.
7. Seleziona Successivo: Revisione. Quando sei pronto, scegli Crea utente.

Migrazione verso autorizzazioni granulari

AWS Artifact ora consente ai clienti di utilizzare autorizzazioni granulari. Grazie a queste autorizzazioni granulari, i clienti avranno un controllo granulare sulla fornitura di accesso a funzionalità come l'accettazione delle condizioni e il download dei report.

Per accedere ai report tramite le autorizzazioni dettagliate, i clienti devono utilizzare la Politica AWSArtifactReportsReadOnlyAccess gestita o aggiornare le proprie autorizzazioni secondo i consigli riportati di seguito. Quindi i clienti devono effettuare l'opt-in utilizzando il collegamento alla pagina dei report di prova del nuovo AWS disponibile nella console.

In caso di problemi con l'aggiornamento alle nuove autorizzazioni, gli utenti avranno la possibilità di accedere ai report con le vecchie autorizzazioni tramite il collegamento alla pagina dei report utilizza la vecchia pagina dei report disponibile nella console.

Migrazione a nuove autorizzazioni

Migrazione delle autorizzazioni non specifiche per le risorse

Gli utenti devono sostituire la politica esistente contenente le autorizzazioni precedenti con una politica contenente autorizzazioni granulari

Politica precedente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/*"
      ]
    }
  ]
}
```

Nuova politica con autorizzazioni dettagliate:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Migrazione delle autorizzazioni specifiche per le risorse

Gli utenti devono sostituire la politica esistente contenente le autorizzazioni precedenti con una politica contenente autorizzazioni granulari. Le autorizzazioni jolly per le risorse dei report sono state sostituite con chiavi condizionali.

Politica precedente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
      ]
    }
  ]
}
```

Nuova politica con autorizzazioni e chiavi di condizione dettagliate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
```

```
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Policy IAM di esempio

Puoi creare politiche di autorizzazione che concedono autorizzazioni agli utenti IAM. Puoi concedere agli utenti l'accesso ai AWS Artifact report e la possibilità di accettare e scaricare gli accordi per conto di un singolo account o di un'organizzazione.

I seguenti esempi di policy mostrano le autorizzazioni che puoi assegnare agli utenti IAM in base al livello di accesso di cui hanno bisogno.

- Esempi di policy per gestire i AWS report con autorizzazioni granulari
- Esempi di politiche per la gestione dei report di terze parti
- Esempi di politiche per la gestione degli accordi
- Politiche di esempio con cui integrarsi AWS Organizations
- Esempi di politiche per la gestione degli accordi per l'account di gestione
- Esempi di politiche per la gestione degli accordi organizzativi
- Esempi di politiche per la gestione delle notifiche

Example Esempi di politiche per gestire i AWS report tramite autorizzazioni granulari

> **Tip**
>
> È consigliabile prendere in considerazione l'utilizzo della politica AWSArtifactReportsReadOnlyAccess gestita anziché definire una politica personalizzata.

La seguente politica concede l'autorizzazione a scaricare tutti i AWS report tramite autorizzazioni granulari.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La seguente politica concede l'autorizzazione a scaricare solo i report AWS SOC, PCI e ISO tramite autorizzazioni dettagliate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
  ]
}
```

Example Esempi di politiche per la gestione dei report di terze parti

> **Tip**
>
> È consigliabile prendere in considerazione l'utilizzo della politica AWSArtifactReportsReadOnlyAccess gestita anziché definire una politica personalizzata.

I report di terze parti sono indicati dalla risorsa `report` IAM.

La seguente politica concede l'autorizzazione a tutte le funzionalità di report di terze parti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

La seguente politica concede l'autorizzazione a scaricare report di terze parti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La seguente politica concede l'autorizzazione a pubblicare report di terze parti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

La seguente politica concede l'autorizzazione a visualizzare i dettagli di un rapporto di terze parti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh"
      ]
    }
  ]
}
```

Example Esempi di politiche per la gestione degli accordi

La seguente politica concede l'autorizzazione a scaricare tutti gli accordi. Gli utenti IAM devono inoltre disporre di questa autorizzazione per accettare gli accordi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede l'autorizzazione ad accettare un accordo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

La seguente politica concede l'autorizzazione a recedere da un contratto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede le autorizzazioni per gestire gli accordi con un singolo account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Example Politiche di esempio con cui integrarsi AWS Organizations

La seguente policy concede l'autorizzazione a creare il ruolo IAM con AWS Artifact AWS Organizationscui effettuare l'integrazione. L'account di gestione dell'organizzazione deve disporre di queste autorizzazioni per iniziare con gli accordi organizzativi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

La seguente politica concede l'autorizzazione a concedere AWS Artifact le autorizzazioni di utilizzo. AWS OrganizationsL'account di gestione dell'organizzazione deve disporre di queste autorizzazioni per iniziare con gli accordi organizzativi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempi di politiche per la gestione degli accordi per l'account di gestione

La seguente politica concede le autorizzazioni per la gestione degli accordi per l'account di gestione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempi di politiche per la gestione degli accordi organizzativi

La seguente politica concede le autorizzazioni per la gestione degli accordi organizzativi. Un altro utente con le autorizzazioni richieste deve configurare gli accordi organizzativi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

La seguente politica concede le autorizzazioni per visualizzare gli accordi organizzativi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Esempi di politiche per la gestione delle notifiche

La seguente politica concede le autorizzazioni complete per l'utilizzo AWS Artifact delle notifiche.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
```

```
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede l'autorizzazione a elencare tutte le configurazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede il permesso di creare una configurazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
```

```
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede il permesso di modificare una configurazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
```

```
    }
  ]
}
```

La seguente politica concede il permesso di eliminare una configurazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede il permesso di visualizzare i dettagli di una configurazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

La seguente politica concede l'autorizzazione a registrare o annullare la registrazione degli hub di notifica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWSpolitiche gestite per AWS Artifact

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono 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 AWSpotrebbero 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 AWSaggiorna 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 AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWSpolitica gestita: AWSArtifactReportsReadOnlyAccess

È possibile allegare la policy `AWSArtifactReportsReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni di *sola lettura* che consentono di elencare, visualizzare e scaricare i report.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `artifact`— Consente ai responsabili di elencare, visualizzare e scaricare report da. AWS Artifact

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Aggiornamenti di Artifact alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Artifact da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia del documento Artifact.

Modifica	Description	Data
Artifact ha iniziato a tracciare le modifiche	Artifact ha iniziato a tenere traccia delle modifiche per le AWS sue politiche gestite e ha introdotto. AWSArtifactReports ReadOnlyAccess	2023-12-15

Utilizzo di ruoli collegati ai servizi per AWS Artifact

AWS Artifact AWS Identity and Access Management utilizza ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad AWS Artifact. I ruoli collegati ai servizi sono predefiniti da AWS Artifact e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica la configurazione di AWS Artifact perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Artifact definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo AWS Artifact può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse AWS Artifact perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

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 al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per AWS Artifact

AWS Artifact utilizza il ruolo collegato al servizio denominato: AWSServiceRoleForArtifactconsente ad AWS Artifact di raccogliere informazioni su un'organizzazione tramite il servizio AWS Organizations.

Il ruolo AWSServiceRoleForArtifact collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `artifact.amazonaws.com`

La policy di autorizzazione dei ruoli denominata AWSArtifactServiceRolePolicy consente ad AWS Artifact di completare le seguenti azioni sulla risorsa. `organizations`

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

Creazione di un ruolo collegato ai servizi per AWS Artifact

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando visiti la scheda Organizations Agreements in un account di gestione dell'organizzazione e selezioni il link «Inizia»AWS Management Console, AWS Artifact crea il ruolo collegato al servizio per te.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando visiti la scheda Organizations Agreements in un account di gestione dell'organizzazione e selezioni il link «Inizia», AWS Artifact crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per AWS Artifact

AWS Artifact non consente di modificare AWSServiceRoleForArtifact 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 al servizio per AWS Artifact

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel 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.

> **Note**
>
> Se il servizio AWS Artifact utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AWS Artifact utilizzate da AWSServiceRoleForArtifact

1. Visita la tabella «Organization Agreements» nella console AWS Artifact
2. Termina tutti gli accordi organizzativi attivi

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAMAWS CLI, o l'AWSAPI per eliminare il ruolo collegato al AWSServiceRoleForArtifact servizio. 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 AWS Artifact

AWS Artifact non supporta l'uso di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Puoi utilizzare il AWSServiceRoleForArtifact ruolo nelle seguenti regioni.

Nome Regione	Identità della regione	Support in AWS Artifact
US East (N. Virginia)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	No
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Sì
Africa (Cape Town)	af-south-1	No
Asia Pacifico (Hong Kong)	ap-east-1	No
Asia Pacifico (Giacarta)	ap-southeast-3	No
Asia Pacific (Mumbai)	ap-south-1	No

Nome Regione	Identità della regione	Support in AWS Artifact
Asia Pacifico (Osaka-Locale)	ap-northeast-3	No
Asia Pacifico (Seoul)	ap-northeast-2	No
Asia Pacific (Singapore)	ap-southeast-1	No
Asia Pacific (Sydney)	ap-southeast-2	No
Asia Pacifico (Tokyo)	ap-northeast-1	No
Canada (Central)	ca-central-1	No
Europe (Frankfurt)	eu-central-1	No
Europa (Irlanda)	eu-west-1	No
Europe (London)	eu-west-2	No
Europa (Milano)	eu-south-1	No
Europe (Paris)	eu-west-3	No
Europa (Stoccolma)	eu-north-1	No
Medio Oriente (Bahrein)	me-south-1	No
Medio Oriente (Emirati Arabi Uniti)	me-central-1	No
Sud America (São Paulo)	sa-east-1	No
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	No
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	No

Utilizzo delle chiavi di condizione IAM

Puoi utilizzare le chiavi di condizione IAM per fornire un accesso granulare ai report su AWS Artifact, in base a categorie e serie di report specifiche.

I seguenti esempi di policy mostrano le autorizzazioni che puoi assegnare agli utenti IAM in base a categorie e serie di report specifiche.

Example Esempi di politiche per la gestione dei AWS report e l'accesso alla lettura

AWS Artifacti report sono indicati dalla risorsa IAM,`report`.

La seguente politica concede il permesso di leggere tutti i AWS Artifact report della `Certifications and Attestations` categoria.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

La seguente politica consente di concedere l'autorizzazione alla lettura di tutti i AWS Artifact report della SOC serie.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

La seguente politica consente di concedere l'autorizzazione alla lettura di tutti i AWS Artifact report ad eccezione di quelli inclusi nella `Certifications and Attestations` categoria.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
```

```
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

Registrazione delle chiamate API AWS Artifact con AWS CloudTrail

AWS Artifactè integrato conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio inAWS Artifact. CloudTrail acquisisce le chiamate API AWS Artifact come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Artifact e le chiamate di codice alle operazioni delle API AWS Artifact. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Artifact Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviataAWS Artifact, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS Artifactinformazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività inAWS Artifact, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS Artifact, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

AWS Artifactsupporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di AWS Artifact

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' GetReportMetadata azione.

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
```

```
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

Cronologia dei documenti per AWS Artifact

La tabella seguente descrive le versioni dei AWS Artifact.

Modifica	Descrizione	Data
Accesso ai report e policy gestite dettagliati AWSArtifactReportReadOnlyAccess	Ha abilitato l'accesso granulare agli Artifact Reports, ha abilitato le chiavi delle condizioni dei report e ha lanciato una policy gestita. AWSArtifactReportsReadOnlyAccess	15 dicembre 2023
Ruolo collegato al servizio AWS Artifact	Aggiunta documentazione sui ruoli collegati ai servizi e policy di esempio aggiornate per l'integrazione di AWS Artifact e AWS Organizations.	26 settembre 2023
Notifiche	Ha pubblicato la documentazione per la gestione delle notifiche e ha apportato aggiornamenti pertinenti alla guida di riferimento dell'API, alla documentazione sulla CloudTrail registrazione e alla pagina AWS Artifact Identity and Access Management.	1° agosto 2023
Report di terze parti - Generalmente disponibili	È stata aggiunta la documentazione di riferimento sull'API, CloudTrail la documentazione di registrazione e reso disponibili a livello generale i report di terze parti.	27 gennaio 2023

Rapporti di terze parti (anteprima)	Sono stati lanciati i report sulla conformità dei fornitori indipendenti di software (ISV) che vendono i loro prodotti. Marketplace AWS Inoltre, sono state aggiunte politiche di esempio alla pagina di gestione delle identità e degli accessi per i report di terze parti.	30 novembre 2022
Sicurezza	È stata aggiunta una sezione alla pagina di gestione delle identità e degli accessi per prevenire la confusione dei deputati.	20 dicembre 2021
Report	È stato rimosso l'accordo di non divulgazione e sono stati introdotti termini e condizioni per il download dei report.	17 dicembre 2020
Home page e ricerca	Sono state aggiunte la home page del servizio e la barra di ricerca nella pagina dei report e degli accordi.	15 maggio 2020
GovCloud avvio	AWS ArtifactLanciato nelle GovCloud regioni.	7 novembre 2019
AWS Organizationsaccordi	È stato aggiunto il supporto per la gestione degli accordi per un'organizzazione.	20 giugno 2018
Accordi	È stato aggiunto il supporto per la gestione AWS Artifact degli accordi.	17 giugno 2017

Versione iniziale	Questa versione introduce AWS Artifact.	30 novembre 2016

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.