Guida per l'utente

AWS Artifact

AWS Artifact: Guida per l’utente

Table of Contents

Che cos'è AWS Artifact?

AWS Artifact fornisce download su richiesta di documenti di AWS sicurezza e conformità. Ad esempio, report sulla conformità agli standard dell'International Organization for Standardization (ISO) e agli standard di sicurezza del settore delle carte di pagamento (PCI) e report sui controlli di sistema e organizzazione (SOC). AWS Artifact fornisce inoltre download delle certificazioni degli organismi di accreditamento che convalidano l'implementazione e l'efficacia operativa dei controlli di sicurezza. AWS

Con AWS Artifact, puoi anche scaricare i documenti di sicurezza e conformità per i fornitori di software indipendenti (ISVs) che vendono i loro prodotti su. Marketplace AWS Per ulteriori informazioni, consulta Marketplace AWS Vendor Insights.

Inoltre, puoi utilizzarli AWS Artifact per esaminare, accettare e monitorare lo stato degli accordi con AWS te Account AWS e per più membri Account AWS dell'organizzazione. Per ulteriori informazioni sugli accordi in AWS Artifact, consultaGestione degli accordi in AWS Artifact.

Per dimostrare la sicurezza e la conformità dell' AWS infrastruttura e dei servizi utilizzati, è possibile inviare AWS Artifact documenti ai revisori o alle autorità di regolamentazione come elementi di controllo. Puoi anche utilizzare questi elementi di audit come linee guida per valutare la tua architettura cloud e per valutare l'efficacia dei controlli interni della tua azienda. Per ulteriori informazioni sugli artefatti di audit, consulta. AWS Artifact FAQs

> **Note**
>
> AWS i 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.

Prezzi

AWS ti fornisce AWS Artifact documenti e accordi gratuitamente.

Guida introduttiva con AWS Artifact

Per iniziare a utilizzarlo AWS Artifact, prova le sue funzionalità principali nella AWS Artifact console. Nella console puoi scaricare report AWS sulla sicurezza e sulla conformità, scaricare e accettare accordi legali e iscriverti alle notifiche sui AWS Artifact documenti.

Prerequisiti

Per utilizzare le funzionalità di AWS Artifact, è necessario disporre di un Account AWS. Per le istruzioni di configurazione, consulta Configurare un nuovo Account AWS nella Guida utente alla AWS configurazione.

Funzionalità

Per istruzioni sull'uso delle funzionalità di AWS Artifact, consulta i seguenti argomenti:

- Scaricamento dei report
- Gestione degli accordi
- Configurazione delle notifiche

Scaricamento dei report in AWS Artifact

Puoi scaricare i report dalla AWS Artifact console. Quando scarichi un rapporto da AWS Artifact, il rapporto viene generato appositamente per te e ogni rapporto ha una filigrana unica. 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

Per scaricare un rapporto, è necessario disporre delle autorizzazioni necessarie. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Quando ti registri AWS Artifact, al tuo account vengono automaticamente concesse le autorizzazioni per scaricare alcuni report. Se riscontri problemi di accesso AWS Artifact, segui le indicazioni 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.

   Nella pagina Rapporti, nella scheda AWS Rapporti, puoi accedere ai AWS report (ad esempio, SOC 1/2/3, PCI, C5 e così via). Nella scheda Rapporti di terze parti, puoi accedere ai report di fornitori di software indipendenti (ISVs) che vendono i propri prodotti. Marketplace AWS
3. (Facoltativo) Per trovare un rapporto, inserisci una parola chiave nel campo di ricerca. Puoi anche eseguire ricerche mirate per i report in base a singole colonne, tra cui titolo, categoria, serie e descrizione del rapporto. Ad esempio, per trovare il rapporto Cloud Computing

Compliance Controls Catalogue (C5), puoi cercare nella colonna Titolo utilizzando «Titolo», l'operatore «contiene» (:) e il termine «C5" (). **`Title : C5`**

4. (Facoltativo) Per ulteriori informazioni su un rapporto, scegli il titolo del rapporto per aprirne la pagina dei dettagli.
5. (Facoltativo) Se desideri scaricare una versione precedente di un rapporto, puoi aprire la pagina dei dettagli del rapporto scegliendo il titolo del rapporto. Nella pagina dei dettagli, cerca la sezione Versioni precedenti e, nella riga della versione desiderata, scegli Scarica per scaricare la versione specifica del rapporto.
6. Seleziona un rapporto, quindi scegli Scarica rapporto.
7. È possibile che ti venga richiesto di accettare i termini e le condizioni (Accetta i termini per scaricare il rapporto) per il rapporto specifico che stai scaricando. Ti consigliamo di leggere attentamente i termini e le condizioni. Al termine della lettura, 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 all'interno del file PDF per la documentazione di supporto. Per istruzioni su come visualizzare gli allegati, consulta. Visualizzazione degli allegati nei documenti PDF

Visualizzazione degli allegati nei documenti PDF

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

Adobe Acrobat Reader

Scarica l'ultima versione di Adobe Acrobat Reader dal sito Web di Adobe all'indirizzo. https://get.adobe.com/reader/

Per istruzioni su come visualizzare gli allegati PDF in Acrobat Reader, consultate Collegamenti e allegati nel sito Web di Adobe PDFs Support.

Browser Firefox

1. Scarica la versione più recente del browser Web Firefox dal sito Web di Mozilla all'indirizzo https://www.mozilla. org/en-US/firefox/new/.

2. Apri il file PDF nel visualizzatore PDF integrato in Firefox. Per istruzioni, consulta Visualizzare i file PDF in Firefox o scegliere un altro visualizzatore sul sito Web di Mozilla Support.
3. Per visualizzare gli allegati PDF nel visualizzatore PDF integrato di Firefox, scegli Attiva/disattiva la barra laterale, Mostra allegati.

Proteggi i tuoi documenti

AWS Artifact i documenti sono riservati e devono essere tenuti al sicuro in ogni momento. AWS Artifact utilizza 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 Artifact potrebbe 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

Puoi utilizzarli AWS Artifact per rivedere e gestire gli accordi per la tua Account AWS organizzazione. Ad esempio, le aziende soggette all'Health Insurance Portability and Accountability Act (HIPAA) in genere richiedono un accordo Business Associate Addendum (BAA) AWS per garantire che le informazioni sanitarie protette (PHI) siano adeguatamente salvaguardate. Nella AWS Artifact console, è possibile esaminare e accettare tali accordi e designare un utente in grado di elaborare legalmente i PHI. Account AWS

Se lo utilizzi AWS Organizations, puoi accettare accordi, ad esempio un BAA con AWS, per conto di tutti i Account AWS membri della tua organizzazione. Tutti gli account membro esistenti e successivi sono automaticamente coperti dall'accordo e possono elaborare giuridicamente i dati sanitari protetti.

Puoi anche AWS Artifact utilizzarlo per confermare che la tua Account AWS organizzazione ha accettato un accordo e per rivedere i termini di un accordo accettato per comprendere i tuoi obblighi. Se il tuo account o la tua organizzazione non devono più utilizzare un 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 riattivare il contratto.

Indice

Accettazione di accordi per tuo conto Account AWSAWS Artifact

Puoi utilizzare la AWS Artifact console per rivedere e accettare gli accordi con AWS for your Account AWS.

> **Important**
>
> 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 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 autorizzazioni richieste.

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Per accettare un accordo con AWS

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nel riquadro AWS Artifact di navigazione, scegli Accordi.
3. Selezionare la scheda Accordi account.
4. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
5. Nel riquadro di navigazione, scegli Accordi.
6. Nella pagina Accordi, esegui una delle seguenti operazioni:
   - Per accettare un contratto solo per il tuo account, scegli la scheda Account agreement.
   - Per accettare un accordo per conto della tua organizzazione, scegli la scheda Accordi organizzativi.
7. Seleziona un contratto, quindi scegli Scarica contratto.

   Viene visualizzata la finestra di dialogo Accetta accordo di non divulgazione per scaricare il rapporto.
8. Prima di poter scaricare l'accordo selezionato, è necessario accettare i termini del Contratto di AWS Artifact non divulgazione (AWS Artifact NDA).

   a. Nella finestra di dialogo Accetta accordo di non divulgazione per scaricare il rapporto, consulta l'accordo di non divulgazione. AWS Artifact
   b. (Facoltativo) Per stampare una copia dell'accordo di AWS Artifact non divulgazione (o salvarlo come PDF), scegli Stampa accordo di non divulgazione.
   c. Seleziona Ho letto e accetto tutti i termini dell'NDA.
   d. Per accettare l'accordo di AWS Artifact non divulgazione e scaricare un PDF del contratto selezionato, scegli Accetta accordo di non divulgazione e scarica.
9. In un visualizzatore PDF, rivedi il PDF dell'accordo che hai scaricato.
10. Nella AWS Artifact console, con l'accordo selezionato, scegli Accetta accordo.

11. Nella finestra di dialogo Accetta accordo, procedi come segue:
    a. Rivedi l'accordo.
    b. Seleziona Accetto tutti questi termini e condizioni.
    c. Scegli Accetta accordo.
12. Scegli Accetta per accettare il contratto per il tuo account.

Risoluzione dei contratti per il tuo account Account AWSAWS Artifact

Se hai utilizzato la AWS Artifact console per accettare un contratto per un singolo utente Account AWS, puoi utilizzare la console per risolvere tale contratto. In caso contrario, consulta Accordi offline in AWS Artifact.

Autorizzazioni richieste

Per recedere da un contratto, IAM e gli utenti federati devono disporre delle autorizzazioni richieste.

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Per recedere dal contratto online con AWS

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

Accettazione di accordi per la tua organizzazione in AWS Artifact

Se sei il proprietario dell'account di gestione di un' AWS Organizations organizzazione, puoi accettare un accordo per AWS conto di tutti i Account AWS membri dell'organizzazione.

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

AWS Organizations ha due set di funzionalità disponibili: funzionalità di fatturazione consolidata e tutte le funzionalità. Per utilizzarlo AWS Artifact per la tua organizzazione, l'organizzazione a cui appartieni deve essere abilitata per tutte le funzionalità. Se la tua organizzazione è configurata solo per la fatturazione consolidata, consulta Abilitazione di tutte le funzionalità dell'organizzazione nella Guida per l'AWS Organizations utente.

Per accettare o rescindere gli accordi organizzativi, devi accedere all'account di gestione con le autorizzazioni corrette. AWS Artifact Gli utenti degli account membro che dispongono `organizations:DescribeOrganization` delle autorizzazioni possono visualizzare gli accordi organizzativi accettati per loro conto.

Per ulteriori informazioni, consulta Gestire gli account in un'organizzazione AWS Organizations nella Guida per l'AWS Organizations utente.

Autorizzazioni richieste

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

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Per accettare un accordo per un'organizzazione

1. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
2. Nella AWS Artifact dashboard, scegli Accordi.
3. Scegliere la scheda Accordi organizzazione.
4. Apri la AWS Artifact console all'indirizzo https://console.aws.amazon.com/artifact/.
5. Nel riquadro di navigazione, scegli Accordi.
6. Nella pagina Accordi, esegui una delle seguenti operazioni:
   - Per accettare un contratto solo per il tuo account, scegli la scheda Account agreement.
   - Per accettare un accordo per conto della tua organizzazione, scegli la scheda Accordi organizzativi.

7. Seleziona un contratto, quindi scegli Scarica contratto.

   Viene visualizzata la finestra di dialogo Accetta accordo di non divulgazione per scaricare il rapporto.

8. Prima di poter scaricare l'accordo selezionato, è necessario accettare i termini del Contratto di AWS Artifact non divulgazione (AWS Artifact NDA).

   a. Nella finestra di dialogo Accetta accordo di non divulgazione per scaricare il rapporto, consulta l'accordo di non divulgazione. AWS Artifact

   b. (Facoltativo) Per stampare una copia dell'accordo di AWS Artifact non divulgazione (o salvarlo come PDF), scegli Stampa accordo di non divulgazione.

   c. Seleziona Ho letto e accetto tutti i termini dell'NDA.

   d. Per accettare l'accordo di AWS Artifact non divulgazione e scaricare un PDF del contratto selezionato, scegli Accetta accordo di non divulgazione e scarica.

9. In un visualizzatore PDF, rivedi il PDF dell'accordo che hai scaricato.

10. Nella AWS Artifact console, con l'accordo selezionato, scegli Accetta accordo.

11. Nella finestra di dialogo Accetta accordo, procedi come segue:

    a. Rivedi l'accordo.

    b. Seleziona Accetto tutti questi termini e condizioni.

    c. Scegli Accetta accordo.

12. Scegli Accetta per accettare l'accordo per tutti gli account esistenti e futuri della tua organizzazione.

Risoluzione degli accordi per la tua organizzazione in AWS Artifact

Se hai utilizzato la AWS Artifact console per accettare un accordo per conto di tutti gli account dei membri di un'organizzazione in AWS Organizations, puoi utilizzare la console per recedere dal contratto. In caso contrario, consulta Accordi offline in AWS Artifact.

Se un account membro viene rimosso da un'organizzazione, tale account membro è più coperto dagli accordi organizzativi. Prima di rimuovere gli account membro da un'organizzazione, l'amministratore dell'account di gestione deve comunicarlo agli account membri in modo che possano stipulare nuovi accordi, se necessario. È possibile visualizzare un elenco degli accordi organizzativi attivi nella AWS Artifact console nella pagina Accordi, in Accordi organizzativi.

Per ulteriori informazioni AWS Organizations, consulta Gestire gli account in un'organizzazione AWS Organizations nella Guida per l'AWS Organizations utente.

Autorizzazioni richieste

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

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

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. Nella AWS Artifact dashboard, scegli 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).

Accordi offline in AWS Artifact

Se disponi di un contratto offline esistente, 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.

Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Configurazione delle notifiche e-mail in AWS Artifact

> **Note**
>
> Il contenuto di questa pagina è applicabile solo alle AWS regioni commerciali e attualmente non si applica a AWS GovCloud (US) Regions.

Puoi utilizzare la AWS Artifact console per configurare le notifiche e-mail per gli aggiornamenti su accordi e report in AWS Artifact. AWS Artifact invia queste notifiche e-mail utilizzando Notifiche all'utente AWS. Per ricevere notifiche AWS Artifact e-mail, devi prima selezionare gli hub di Notifiche all'utente AWS notifica nella Notifiche all'utente console. Quindi, nella AWS Artifact console, è possibile creare una configurazione per le impostazioni di notifica, in cui specificare i destinatari delle notifiche e le notifiche che ricevono.

Per configurare le notifiche AWS Artifact e-mail, è necessario disporre delle autorizzazioni richieste per AWS Artifact e. Notifiche all'utente AWS Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Artifact.

Indice

Prerequisito: selezionare gli hub di notifica in Notifiche all'utente

Prima di poter ricevere notifiche AWS Artifact e-mail, è necessario aprire la Notifiche all'utente console e selezionare gli hub di notifica in Regioni AWS cui si desidera archiviare i dati. Notifiche all'utente È necessario selezionare gli hub di notifica Notifiche all'utente AWS, che vengono AWS Artifact utilizzati per inviare notifiche.

Per selezionare gli hub di notifica

1. Apri la pagina degli hub di notifica della Notifiche all'utente AWS console.

2. Seleziona gli hub di notifica in Regioni AWS cui desideri archiviare le tue Notifiche all'utente AWS risorse. Per impostazione predefinita, i Notifiche all'utente dati vengono archiviati nella regione Stati Uniti orientali (Virginia settentrionale). Notifiche all'utente replica i dati delle notifiche nelle altre regioni selezionate. Per ulteriori informazioni, consulta la documentazione sugli hub di notifica nella Guida per l'Notifiche all'utente AWS utente.
3. Seleziona Salva e continua.

Creazione di una configurazione per le impostazioni AWS Artifact di notifica

> **Note**
>
> Il contenuto di questa pagina è applicabile solo alle AWS regioni commerciali e attualmente non si applica a AWS GovCloud (US) Regions.

Dopo aver selezionato gli hub di Notifiche all'utente notifica, è possibile creare una configurazione per le impostazioni di notifica nella AWS Artifact console. Nella configurazione creata, specifichi gli indirizzi e-mail dei destinatari a cui desideri ricevere AWS Artifact le notifiche. Specificate inoltre per quali aggiornamenti tali destinatari devono ricevere notifiche, ad esempio aggiornamenti per gli AWS Artifact accordi e aggiornamenti per tutti i report (o un sottoinsieme di) AWS Artifact .

Per creare una configurazione

1. Apri la pagina delle impostazioni di notifica della AWS Artifact console.
2. Scegli Crea configurazione.
3. Nella pagina Crea configurazione, procedi come segue:
   - Per ricevere notifiche relative agli accordi, in Accordi, mantieni selezionata l'opzione Aggiornamenti sugli AWS accordi.
   - Per ricevere notifiche relative ai report, in Report, mantieni selezionata l'opzione Aggiornamenti sui AWS report.
     a. Per ricevere notifiche per tutti i report, scegli Tutti i report.
     b. Per ricevere notifiche solo per i report rientranti in categorie e serie specifiche, scegli Un sottoinsieme di report. Quindi, seleziona le categorie e le serie che ti interessano.

- In Nome di configurazione, inserisci un nome per la tua configurazione.
- In E-mail, per Destinatari, inserisci un elenco separato da virgole di indirizzi e-mail a cui desideri ricevere e-mail di notifica. AWS Artifact
- (Facoltativo) Per aggiungere tag alla configurazione delle notifiche, espandi Tag, scegli Aggiungi nuovo tag, quindi inserisci i tag come coppie chiave-valore. Per ulteriori informazioni sull'etichettatura Notifiche all'utente delle risorse, consulta Etichettare le Notifiche all'utente AWS risorse nella Guida per l'utente.Notifiche all'utente AWS
- Scegli Crea configurazione.

  Notifiche all'utente invia un'email di verifica a ciascuno degli indirizzi e-mail dei destinatari che hai fornito. Per verificare l'indirizzo e-mail, nell'e-mail di verifica, il destinatario deve scegliere Verifica email. Solo gli indirizzi email verificati riceveranno AWS Artifact le notifiche.

Modifica di una configurazione per le impostazioni AWS Artifact di notifica

> **Note**
>
> Il contenuto di questa pagina è applicabile solo alle AWS regioni commerciali e attualmente non si applica a AWS GovCloud (US) Regions.

Dopo aver creato una configurazione per le impostazioni di AWS Artifact notifica, è possibile modificare la configurazione in qualsiasi momento per modificare le impostazioni di notifica. Ad esempio, per aggiungere o rimuovere destinatari, modificare i tipi di notifiche che ricevono e aggiungere o rimuovere tag.

Per modificare una configurazione

1. Apri la pagina delle impostazioni di notifica della AWS Artifact console.
2. Seleziona la configurazione che desideri modificare.
3. Scegli Modifica.
4. Modifica tutte le selezioni e i campi di configurazione. Quando hai finito, scegli Salva modifiche.

Se hai aggiunto nuovi indirizzi e-mail come destinatari delle notifiche, Notifiche all'utente AWS invia un'email di verifica a tali indirizzi e-mail. Per verificare l'indirizzo e-mail, nell'e-mail di verifica, il destinatario deve scegliere Verifica email. Solo gli indirizzi email verificati riceveranno AWS Artifact le notifiche.

Eliminazione di una configurazione per le impostazioni di AWS Artifact notifica

> **Note**
>
> Il contenuto di questa pagina è applicabile solo alle AWS regioni commerciali e attualmente non si applica a AWS GovCloud (US) Regions.

Se non è più necessaria una configurazione creata per le impostazioni di AWS Artifact notifica, è possibile eliminare la configurazione nella AWS Artifact console.

Per eliminare una configurazione

1. Apri la pagina delle impostazioni di notifica della AWS Artifact console.
2. Seleziona la configurazione che desideri eliminare.
3. Scegli Elimina.
4. Nella finestra di dialogo Elimina configurazione, scegliete Elimina.

Gestione delle identità e degli accessi in AWS Artifact

Quando ti registri AWS, fornisci un indirizzo email e una password associati al tuo AWS account. Queste sono le tue credenziali di root e forniscono l'accesso completo a tutte le tue AWS risorse, incluse le risorse per AWS 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'esterno AWS, 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

Concessione all'utente dell'accesso a AWS Artifact

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

Attività

- 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 riquadro di navigazione, scegli 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 diEsempi di politiche IAM per AWS Artifact le AWS regioni commerciali.
6. Scegli Esamina la 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 Create Policy (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 Console di gestione AWS . 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. Scegli Successivo: Tag. Facoltativamente, puoi aggiungere tag ai tuoi utenti.
7. Scegli Prossimo: Rivedi. Quando sei pronto, scegli Crea utente.

Esempi di politiche IAM per AWS Artifact le AWS regioni commerciali

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.

Queste politiche sono applicabili nelle regioni commerciali AWS . Per le politiche applicabili a AWS GovCloud (US) Regions, consulta Esempi di politiche IAM per AWS Artifact in AWS GovCloud (US) Regions

- Esempi di politiche 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 AWSArtifact ReportsReadOnlyAccess 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",
        "artifact:ListReportVersions"
      ],
      "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"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "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 AWSArtifact ReportsReadOnlyAccess 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 elencare report di terze parti.

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

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

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

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

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

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

> **Tip**
>
> È consigliabile prendere in considerazione l'utilizzo della politica AWSArtifactAgreementsReadOnlyAccess o della politica AWSArtifact AgreementsFullAccess gestita anziché definire la propria politica.

Example Esempi di politiche per la gestione degli accordi

La seguente politica concede l'autorizzazione a scaricare tutti gli accordi.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
```

```
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

La seguente politica concede l'autorizzazione ad accettare tutti gli accordi.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
```

```
}
```

La seguente politica concede l'autorizzazione a risolvere tutti gli accordi.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

La seguente politica concede le autorizzazioni per visualizzare ed eseguire accordi a livello di account.

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

```
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-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 Organizations cui 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": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
```

```
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

La seguente politica concede l'autorizzazione a concedere AWS Artifact le autorizzazioni di utilizzo. AWS Organizations 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": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   },
   {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
```

```
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
 ]
}
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
```

```
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
```

```
  ]
}
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
```

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

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

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-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": [
        "*"
      ]
    }
  ]
}
```

Esempi di politiche IAM per in AWS ArtifactAWS GovCloud (US) Regions

Queste politiche sono applicabili SOLO in AWS GovCloud (US) Regions. Per le politiche applicabili alle AWS regioni commerciali, consulta Esempi di politiche IAM per AWS Artifact le AWS regioni commerciali

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 report AWS
- 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

Example Esempi di politiche per la gestione dei report

La seguente politica concede il permesso di scaricare tutti i report.

```
{
  "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 SOC, PCI e ISO.

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

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:ListAgreements",
        "artifact:ListCustomerAgreements"
```

```
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

La seguente politica concede il permesso di accettare tutti gli accordi.

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    }
  ]
}
```

La seguente politica concede il permesso di risolvere tutti i contratti.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

La seguente politica concede le autorizzazioni per visualizzare ed eseguire accordi a livello di account.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-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 Organizations cui 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": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

La seguente politica concede l'autorizzazione a concedere AWS Artifact le autorizzazioni di utilizzo. AWS Organizations 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": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EnableServiceTrustForArtifact",
```

```
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "aws-artifact-account-sync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
```

```
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
  ]
}
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

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

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
```

```
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Utilizzo di politiche AWS gestite per AWS Artifact

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti 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 politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

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

AWS politica gestita: AWSArtifactReportsReadOnlyAccess

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

Questa politica concede *`read-only`* autorizzazioni 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 i report da. AWS Artifact

AWS politica gestita: AWSArtifactAgreementsReadOnlyAccess

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

Questa policy *`read-only`* consente l'accesso all'elenco degli accordi di servizio AWS Artifact e al download degli accordi accettati. Include anche le autorizzazioni per elencare e descrivere i dettagli dell'organizzazione. Inoltre, la policy offre la possibilità di verificare se esiste il ruolo collegato al servizio richiesto.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `artifact`— Consente ai mandanti di elencare tutti gli accordi e di visualizzare gli accordi accettati da. AWS Artifact
- `iam`— Consente ai dirigenti di verificare se esiste il ruolo collegato al servizio richiesto.
- `organizations`— Consente ai dirigenti di descrivere l'organizzazione corrente e di elencare gli accessi ai servizi per quell'organizzazione.

AWS politica gestita: AWSArtifactAgreementsFullAccess

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

Questa policy concede *full* le autorizzazioni per elencare, scaricare, accettare e terminare gli accordi AWS Artifact. Include anche le autorizzazioni per elencare e abilitare l'accesso ai servizi AWS nel AWS Organizations servizio, oltre a descrivere i dettagli dell'organizzazione. Inoltre, la policy offre la possibilità di verificare se esiste il ruolo collegato al servizio richiesto e di crearne uno in caso contrario.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `artifact`— Consente ai responsabili di elencare, scaricare, accettare e rescindere gli accordi da. AWS Artifact
- `iam`— Consente ai responsabili di verificare se esiste il ruolo collegato al servizio richiesto e di crearne uno in caso contrario.
- `organizations`— Consente ai dirigenti di descrivere l'organizzazione attuale e l'accesso ai list/enable servizi per tale organizzazione.

AWS Artifact aggiornamenti alle politiche AWS gestite

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

Modifica	Descrizione	Data
Policy gestite aggiornate di AWS Agreements	Politica AWSArtifact AgreementsFullAccess gestita aggiornata per limitare `organizations:EnableAWSServiceAccess` le autorizzazioni al responsabile AWS Artifact del servizio. Ciò non influisce sulla funzionalità della policy gestita.	2025-10-16

Modifica	Descrizione	Data
Policy gestite aggiornate di AWS Reports	Policy AWSArtifact ReportsReadOnlyAccess gestita aggiornata per rimuovere l'artefatto: get permission.	2025-03-21
Introdotte le politiche gestite di AWS Agreements	Politiche introdotte AWSArtifact AgreementsReadOnlyAccess e AWSArtifact AgreementsFullAccess gestite.	2024-11-21
AWS Artifact ha iniziato a tenere traccia delle modifiche	AWS Artifact ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite e ha introdotto AWSArtifactReportsReadOnlyAccess.	15/12/23

Utilizzo di ruoli collegati ai servizi per AWS Artifact

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

Un ruolo collegato al servizio semplifica la configurazione AWS Artifact perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Artifact definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Artifact 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. In questo modo proteggi AWS Artifact le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. 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 AWSServiceRoleForArtifact: consente di AWS Artifact raccogliere informazioni su un'organizzazione tramite. AWS Organizations

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

- `artifact.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSArtifact ServiceRolePolicy consente di AWS Artifact completare le seguenti azioni sulla risorsa. `organizations`

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

Creazione di un ruolo collegato al servizio per AWS Artifact

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando accedi alla scheda Accordi organizzativi in un account di gestione dell'organizzazione e scegli il link Guida introduttiva in Console di gestione AWS, AWS Artifact crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando accedi alla scheda Accordi organizzativi in un account di gestione dell'organizzazione e scegli il link Inizia, AWS Artifact crea nuovamente il ruolo collegato al servizio.

Modifica di un ruolo collegato al servizio per AWS Artifact

AWS Artifact non consente di modificare il ruolo collegato al AWSService RoleForArtifact 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 AWS Artifact servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS Artifact le risorse utilizzate da AWSService RoleForArtifact

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

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSService RoleForArtifact 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'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. È possibile utilizzare il AWSService RoleForArtifact ruolo nelle seguenti regioni.

Nome della 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

Nome della Regione	Identità della regione	Support in AWS Artifact
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
Asia Pacifico (Osaka-Locale)	ap-northeast-3	No
Asia Pacifico (Seul)	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

Nome della Regione	Identità della regione	Support in AWS Artifact
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	No
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	Sì

Utilizzo delle chiavi di condizione IAM per i report AWS Artifact

Puoi utilizzare le chiavi di condizione IAM per fornire un accesso granulare ai report 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 Artifact i 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 della `Certifications and Attestations` categoria e 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"
        }
      }
    }
  ]
}
```

Registrazione delle chiamate AWS Artifact API con AWS CloudTrail

AWS Artifact è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Artifact. CloudTrail acquisisce le chiamate API AWS Artifact come eventi. Le chiamate acquisite includono chiamate dalla AWS Artifact console e chiamate di codice alle operazioni AWS Artifact API. 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 inviata AWS 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 Artifact informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS 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 eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo sito Account AWS, inclusi gli eventi di AWS Artifact, crea un percorso. 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 trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail 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 Artifact supporta la registrazione delle seguenti azioni come eventi nei file di CloudTrail registro:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

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 AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle AWS Artifact voci dei file di registro

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 fornisce una cronologia delle AWS Artifact versioni e delle relative modifiche alla Guida per l' AWS Artifact utente.

Modifica	Descrizione	Data
Politica AWSArtifact AgreementsFullAccess gestita aggiornata	Politica AWSArtifactReports ReadOnlyAccessgestita aggiornata per limitare `organizations:EnableAWSServiceAccess` le autorizzazioni al principale AWS Artifact del servizio. Ciò non influisce sulla funzionalità della policy gestita.	16 ottobre 2025
Aggiornamento dell'avviso di deprecazione di IAM Action	È stato aggiornato l'avviso di deprecazione delle azioni IAM per e nella partizione. `artifact:DownloadAgreement artifact:Get` AWS GovCloud (US)	1 luglio 2025
Autorizzazioni dettagliate per in AWS ArtifactAWS GovCloud (US) Regions	I criteri aggiornati ed estesi per l'utilizzo AWS Artifact in AWS GovCloud (US) Regions, pur eliminando le note sulle limitazioni, sono ora applicabili in modo più ampio in AWS Artifact tutte le aree geografiche.	31 marzo 2025
Politica AWSArtifact ReportReadOnlyAccess gestita aggiornata	Politica AWSArtifactReports ReadOnlyAccessgestita aggiornata per rimuovere l'artefatto:get permission.	21 marzo 2025

Politiche di esempio per in AWS ArtifactAWS GovCloud (US) Regions	Sono state aggiunte politiche di esempio per l'utilizzo AWS Artifact in AWS GovCloud (US) Regions e sono state annotate quali pagine non si applicano all'utilizzo AWS Artifact in AWS GovCloud (US) Regions.	6 dicembre 2024
Autorizzazioni dettagliate per l'esecuzione degli accordi e le politiche gestite AWSArtifact AgreementsFullAccess AWSArtifact AgreementsReadOnlyAccess	Ha consentito l'accesso granulare per l'esecuzione degli AWS Artifact accordi e le politiche avviate e gestite. AWSArtifact AgreementsFullAccess AWSArtifact AgreementsReadOnlyAccess AWS	21 novembre 2024
Accesso granulare ai report e policy gestite AWSArtifact ReportReadOnlyAccess	Ha consentito l'accesso granulare ai report, ha abilitato i codici delle condizioni AWS Artifact dei report e ha lanciato una politica gestita. AWSArtifact ReportsReadOnlyAccess	15 dicembre 2023
AWS Artifact ruolo collegato al servizio	È stata aggiunta la documentazione sui ruoli collegati ai servizi e le politiche di esempio aggiornate per l'integrazione. AWS Artifact AWS Organizations	26 settembre 2023

Notifiche	Ha pubblicato la documentazione per la gestione delle notifiche e ha apportato gli aggiornamenti pertinenti all' AWS Artifact API Reference , alla documentazione sulla CloudTrail registrazione e alla pagina di gestione delle identità e degli accessi.	1° agosto 2023
Rapporti di terze parti: generalmente disponibili	Sono stati aggiunti la documentazione di riferimento sulle API e CloudTrail la documentazione di registrazione e reso disponibili a tutti i report di terze parti.	27 gennaio 2023
Rapporti di terze parti (anteprima)	Sono stati lanciati i report sulla conformità dei fornitori di software indipendenti (ISVs) che vendono i loro prodotti. Marketplace AWS Sono stati aggiunti esempi di policy 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
AWS GovCloud (US) avvio	Lanciato AWS Artifact nel AWS GovCloud (US) Regions.	7 novembre 2019
AWS Organizations accordi	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.