aws

Guida per l'utente

Gestione audit AWS

Gestione audit AWS: Guida per l’utente

Table of Contents

Che cos'è AWS Audit Manager?

Benvenuto nella Guida per AWS Audit Manager l'utente.

AWS Audit Manager ti aiuta a controllare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore. Gestione audit automatizza la raccolta delle prove per consentire di valutare più facilmente se le policy, le procedure e le attività, note anche come controlli, funzionino in modo efficace. Quando è il momento di effettuare un audit, Gestione audit aiuta a gestire le revisioni dei controlli effettuati dalle parti interessate. Ciò significa che è possibile creare report pronti per l'audit con molto meno sforzo manuale.

Gestione audit fornisce framework predefiniti che strutturano e automatizzano le valutazioni in base a un determinato standard o regolamento di conformità. I framework includono una raccolta predefinita di controlli con descrizioni e procedure di test. I controlli sono raggruppati in base ai requisiti dello standard o del regolamento di conformità specificato. È inoltre possibile personalizzare framework e controlli per supportare gli audit interni in base ai requisiti specifici.

È possibile creare una valutazione da qualsiasi framework. Quando si crea una valutazione, Gestione audit esegue automaticamente le valutazioni delle risorse. Queste valutazioni raccolgono dati per i Account AWS settori da voi definiti rientranti nell'ambito dell'audit. I dati raccolti vengono trasformati automaticamente in prove idonee all'audit. Dopodiché vengono collegati ai controlli pertinenti per consentire di dimostrare la conformità in materia di sicurezza, gestione delle modifiche, continuità aziendale e licenze software. Il processo di raccolta delle prove è continuo e inizia nel momento in cui si crea una valutazione. Dopo aver completato un audit e non avendo più bisogno di Gestione audit per raccogliere le prove, è possibile interrompere la raccolta delle prove. Per farlo, occorre modificare lo stato della valutazione in Inattiva.

Funzionalità di Gestione audit

Con AWS Audit Manager, puoi eseguire le seguenti attività:

- Inizia subito: crea la tua prima valutazione selezionando da una galleria di framework predefiniti che supportano una serie di standard e normative di conformità. Quindi, avvia la raccolta automatica delle prove per verificarne Servizio AWS l'utilizzo.
- Carica e gestisci le prove da ambienti ibridi o multicloud: oltre alle prove che Gestione audit raccoglie dal tuo ambiente AWS , puoi anche caricare e gestire centralmente le prove dal tuo ambiente on-premise o multicloud.

- Supporta standard e normative di conformità comuni: scegli uno dei AWS Audit Manager framework standard. Questi framework forniscono mappature di controllo predefinite per standard e regolamenti di conformità comuni. Questi includono CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA, SOC2, GxP e le migliori pratiche operative. AWS
- Monitora le valutazioni attive: utilizza la dashboard di Gestione audit per visualizzare i dati di analisi per le valutazioni attive e identificare rapidamente le prove non conformi che devono essere corrette.
- Cerca prove: utilizza la Evidence finder funzione per trovare rapidamente prove pertinenti alla tua query di ricerca. Puoi generare un report di valutazione in base ai risultati della ricerca, o esportare i risultati della ricerca in formato CSV.
- Crea controlli personalizzati: crea il tuo controllo da zero o crea una copia modificabile di un controllo standard o personalizzato esistente. Puoi anche utilizzare la funzionalità di controlli personalizzati per creare domande di valutazione del rischio e memorizzare le risposte a tali domande come prove manuali.
- Mappa i controlli aziendali su raggruppamenti predefiniti di fonti di AWS dati: scegli i controlli comuni che rappresentano i tuoi obiettivi e usali per creare controlli personalizzati che raccolgono prove del tuo portafoglio di esigenze di conformità.
- Crea framework personalizzati: crea i tuoi framework con controlli standard o personalizzati in base ai tuoi requisiti specifici per gli audit interni.
- Condividi framework personalizzati: condividi i tuoi framework Audit Manager personalizzati con un altro Account AWS utente o replicali in un altro Regione AWS con il tuo account.
- Supporta la collaborazione tra team: delega i set di controlli a esperti in materia che possano esaminare le prove correlate, aggiungere commenti e aggiornare lo stato di ciascun controllo.
- Crea report per i revisori: genera report di valutazione che riassumono le prove pertinenti raccolte per l'audit e collegale a cartelle che contengono le prove dettagliate.
- Garantisci l'integrità delle prove: memorizza le prove in un luogo sicuro, dove rimarranno inalterate.

> **Note**
>
> AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e regolamenti di conformità. Tuttavia, non viene eseguita la valutazione della conformità. AWS Audit Manager Pertanto, le prove raccolte potrebbero non includere tutte le informazioni sull' AWS utilizzo necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Prezzi di Gestione audit

Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Audit Manager.

È la prima volta che utilizzi Gestione audit?

Se utilizzi Gestione audit per la prima volta, ti consigliamo di iniziare dalle seguenti pagine:

1. Comprensione dei concetti e della terminologia AWS Audit Manager— Scopri i concetti e i termini chiave utilizzati in Audit Manager, come valutazioni, framework e controlli.
2. Comprendere come AWS Audit Manager raccogliere le prove— Scopri come Audit Manager raccoglie prove per una valutazione delle risorse.
3. Configurazione AWS Audit Manager con le impostazioni consigliate— Scopri i requisiti di configurazione per Audit Manager.
4. Iniziare con AWS Audit Manager— Segui un tutorial per creare la tua prima valutazione di Audit Manager.
5. AWS Audit Manager Riferimento all'API: acquisisci familiarità con le azioni e i tipi di dati dell'API Audit Manager.

Altre risorse Gestione audit

Le risorse seguenti forniscono ulteriori informazioni su Gestione audit.

- Raccogli prove e gestisci i dati di audit utilizzando AWS Audit Manager
- Integrazione attraverso il modello a tre linee (parte 2): trasforma i pacchetti di AWS Config conformità in AWS Audit Manager valutazioni tratte dal blog AWS Management & Governance

Comprensione dei concetti e della terminologia AWS Audit Manager

Per aiutarti a iniziare, questa pagina definisce i termini e spiega alcuni dei concetti chiave di AWS Audit Manager.

A

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Valutazione

È possibile utilizzare una valutazione di Gestione audit per raccogliere automaticamente le prove pertinenti per un audit.

Una valutazione si basa su un framework, che è un raggruppamento di controlli correlati all'audit. Puoi creare una valutazione da un framework standard o da un framework personalizzato. I framework standard contengono set di controlli predefiniti che supportano uno standard o una normativa di conformità specifici. Al contrario, i framework personalizzati contengono controlli che è possibile personalizzare e raggruppare in base ai requisiti di audit specifici. Utilizzando un framework come punto di partenza, è possibile creare una valutazione che specifichi Account AWS ciò che si desidera includere nell'ambito dell'audit.

Quando si crea una valutazione, Audit Manager inizia automaticamente a valutare le risorse in uso in Account AWS base ai controlli definiti nel framework. Successivamente, raccoglie le prove pertinenti e le converte in un formato adatto ai revisori. Dopo aver fatto ciò, allega le prove ai controlli della valutazione. Quando è il momento di un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte e aggiungerle a un report di valutazione. Il report di valutazione aiuta a dimostrare che i controlli funzionano come previsto.

Il processo di raccolta delle prove è continuo e inizia nel momento in cui si crea una valutazione. Puoi interrompere la raccolta delle prove modificando lo stato della valutazione in Inattivo. In alternativa, puoi interrompere la raccolta delle prove a livello di controllo. Per farlo, modifica lo stato di un controllo specifico all'interno della tua valutazione in Inattivo.

Per istruzioni su come creare e gestire le valutazioni, consulta Gestione delle valutazioni in AWS Audit Manager.

Report di valutazione

Un report di valutazione è un documento definitivo generato da una valutazione di Gestione audit. I report riassumono le prove pertinenti raccolte per l'audit. Si collegano alle cartelle delle prove pertinenti. Le cartelle sono denominate e organizzate in base ai controlli specificati nella valutazione. Per ogni valutazione, è possibile esaminare le prove raccolte da Gestione audit e decidere quali prove includere nel report di valutazione.

Per ulteriori informazioni sui report di valutazione, consulta Report di valutazione. Per informazioni su come generare un report di valutazione, consulta Preparazione di un rapporto di valutazione in AWS Audit Manager.

Destinazione del report di valutazione

La destinazione dei report di valutazione è il bucket S3 predefinito in cui Gestione audit salva i report di valutazione. Per ulteriori informazioni, consulta Configurazione della destinazione predefinita del rapporto di valutazione.

Audit

Un audit è un esame indipendente delle risorse, delle operazioni o dell'integrità aziendale dell'organizzazione. Un audit informatico (IT) esamina specificamente i controlli all'interno dei sistemi informativi dell'organizzazione. L'obiettivo di un audit IT è determinare se i sistemi informativi salvaguardino le risorse, funzionino in modo efficace e mantengano l'integrità dei dati. Tutti questi aspetti sono importanti per soddisfare i requisiti normativi imposti da uno standard o da un regolamento di conformità.

Proprietario dell'audit

Il termine proprietario dell'audit assume due significati diversi a seconda del contesto.

Nel contesto di Gestione audit, il proprietario dell'audit è un utente o un ruolo che gestisce una valutazione e le relative risorse. Le responsabilità di questo Gestione audit includono la creazione di valutazioni, la revisione delle prove e la generazione di report di valutazione. Gestione audit è un servizio collaborativo e i proprietari degli audit traggono vantaggio dalla partecipazione di altre parti interessate alle loro valutazioni. Ad esempio, è possibile aggiungere altri proprietari dell'audit alla valutazione per condividere le attività di gestione. In alternativa, se sei titolare di un audit e hai bisogno di aiuto per interpretare le prove raccolte per un controllo, puoi delegare tale set di controlli a una parte interessata con esperienza specifica in quell'area. Tale persona è nota come persona delegata.

In termini commerciali, il proprietario dell'audit è una persona che coordina e supervisiona gli sforzi di preparazione all'audit della propria azienda e presenta le prove a un revisore. In genere, si tratta di un professionista della governance, del rischio e della conformità (GRC), come un responsabile della conformità o un responsabile della protezione dei dati GDPR. I professionisti GRC hanno l'esperienza e l'autorità necessarie per gestire la preparazione degli audit. Più specificamente, comprendono i requisiti di conformità e possono analizzare, interpretare e preparare i dati di reporting. Tuttavia, anche altre figure aziendali possono assumere il ruolo di Gestione audit di un proprietario dell'audit, non solo i professionisti GRC. Ad esempio, potresti scegliere di far configurare e gestire le valutazioni di Gestione audit da un esperto tecnico di uno dei seguenti team:

- SecOps

- IT/ DevOps
- Centro operativo di sicurezza/risposta agli incidenti
- Team simili che possiedono, sviluppano, rimediano e distribuiscono risorse cloud e comprendono l'infrastruttura cloud della tua organizzazione

La persona scelta come proprietario dell'audit nella valutazione di Gestione audit dipende molto dall'organizzazione. Dipende anche da come si strutturano le operazioni di sicurezza e dalle specifiche dell'audit. In Gestione audit, la stessa persona può assumere il ruolo di proprietario dell'audit in una valutazione e il ruolo di delegato in un'altra.

Indipendentemente dal modo in cui si sceglie di utilizzare Gestione audit, è possibile gestire la separazione dei compiti all'interno dell'organizzazione utilizzando la persona del proprietario/delegato dell'audit e assegnando policy IAM specifiche a ciascun utente. Grazie a questo approccio in due fasi, Gestione audit garantisce il pieno controllo su tutte le specifiche di una valutazione individuale. Per ulteriori informazioni, consulta Politiche consigliate per gli utenti in AWS Audit Manager.

AWS fonte gestita

Una fonte AWS gestita è una fonte di prove che AWS conserva per te.

Ogni fonte AWS gestita è un raggruppamento predefinito di fonti di dati che si associa a uno specifico controllo comune o controllo principale. Quando si utilizza un controllo comune come fonte di prove, si raccolgono automaticamente le prove per tutti i controlli principali che supportano tale controllo comune. Puoi anche utilizzare i singoli controlli di base come fonte di prove.

Ogni volta che una fonte AWS gestita viene aggiornata, gli stessi aggiornamenti vengono applicati automaticamente a tutti i controlli personalizzati che utilizzano tale fonte AWS gestita. Ciò significa che i controlli personalizzati raccolgono prove in base alle definizioni più recenti di quella fonte di prove. Questo ti aiuta a garantire una conformità continua man mano che l'ambiente di conformità cloud cambia.

Vedi anche:customer managed source,evidence source.

C

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Changelog

Per ogni controllo in una valutazione, Audit Manager tiene traccia delle attività degli utenti per quel controllo. È quindi possibile esaminare un audit trail delle attività correlate a un controllo specifico. Per ulteriori informazioni sulle attività degli utenti registrate nel changelog, vedere. Scheda Changelog

Conformità cloud

La conformità cloud è il principio generale secondo cui i sistemi forniti nel cloud devono essere conformi agli standard richiesti dai clienti del cloud.

Controllo comune

Per informazioni, consulta control.

Regolamento di conformità

Un regolamento di conformità è una legge, una norma o un altro ordine prescritto da un'autorità, in genere per regolare una condotta. Un esempio è GDPR.

Standard di conformità

Uno standard di conformità è un insieme strutturato di linee guida che descrivono in dettaglio i processi di un'organizzazione per mantenere la conformità ai regolamenti, alle specifiche o alla legislazione stabiliti. Gli esempi comprendono PCI DSS e HIPAA.

Controllo

Un controllo è una misura di salvaguardia o contromisura prescritta per un sistema informativo o un'organizzazione. I controlli sono progettati per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e per soddisfare una serie di requisiti definiti. Garantiscono che le risorse funzionino come previsto, che i dati siano affidabili e che l'organizzazione sia conforme alle leggi e ai regolamenti applicabili.

In Gestione audit, un controllo può anche rappresentare una domanda in un questionario di valutazione del rischio del fornitore. In questo caso, un controllo è una domanda specifica che richiede informazioni sul livello di sicurezza e conformità di un'organizzazione.

I controlli raccolgono continuamente prove quando sono attivi nelle valutazioni di Gestione audit. È anche possibile aggiungere manualmente prove a qualsiasi controllo. Ogni elemento di prova è un documento che consente di dimostrare la conformità ai requisiti del controllo.

Audit Manager fornisce i seguenti tipi di controlli:

Tipo di controllo	Descrizione
Controllo comune	Puoi pensare a un controllo comune come a un'azione che ti aiuta a raggiunge re un obiettivo di controllo. Poiché i controlli comuni non sono specifici di nessuno standard di conformità, consentono di raccogliere prove a supporto di una serie di obblighi di conformità sovrapposti. Ad esempio, supponiamo di avere un obiettivo di controllo chiamato Classific azione e gestione dei dati. Per raggiungere questo obiettivo, è possibile implementare un controllo comune chiamato Controlli di accesso per monitorar e e rilevare gli accessi non autorizzati alle risorse. • I controlli comuni automatizzati raccolgono prove per te. Sono costituiti da un raggruppamento di uno o più controlli principali correlati. A sua volta, ciascuno di questi controlli principali raccoglie automaticamente le prove pertinenti da un gruppo predefinito di fonti di AWS dati. AWS gestisce queste fonti di dati sottostanti per te e le aggiorna ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati. • I controlli manuali comuni richiedono il caricamento delle proprie prove. Questo perché in genere richiedono la fornitura di registrazioni fisiche o dettagli sugli eventi che si verificano al di fuori AWS dell'ambiente. Per questo motivo, spesso non esistono fonti di AWS dati in grado di fornire prove a sostegno dei requisiti comuni di controllo manuale. Non è possibile modificare un controllo comune. Tuttavia, puoi utilizzare qualsiasi controllo comune come fonte di prova quando crei un controllo personalizzato.
Controllo di base	Si tratta di una linea guida prescrittiva per il vostro ambiente. AWS È possibile pensare a un controllo di base come a un'azione che consente di soddisfare i requisiti di un controllo comune. Ad esempio, supponiamo che tu utilizzi un controllo comune chiamato Controlli di accesso per monitorare l'accesso non autorizzato alle tue risorse. Per supportare questo controllo comune, puoi utilizzare il controllo principale chiamato Blocca l'accesso pubblico alla lettura nei bucket S3.

Tipo di controllo	Descrizione
	Poiché i controlli di base non sono specifici per nessuno standard di conformità, raccolgono prove che possono supportare una serie di obblighi di conformità sovrapposti. Ogni controllo principale utilizza una o più fonti di dati per raccogliere prove su uno specifico. Servizio AWS AWS gestisce queste fonti di dati sottostanti per te e le aggiorna ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati. Non puoi modificare un controllo principale. Tuttavia, puoi utilizzare qualsiasi controllo di base come fonte di prova quando crei un controllo personalizzato.
Controllo standard	Si tratta di un controllo predefinito fornito da Audit Manager. È possibile utilizzare i controlli standard per assistervi nella preparazione degli audit per uno specifico standard di conformità. Ogni controllo standard è correlato a uno standard specifico framework in Audit Manager e raccoglie prove che è possibile utilizzare per dimostrare la conformità a tale framework . I controlli standard raccolgono prove dalle fonti di dati sottostanti che AWS gestisce. Queste fonti di dati vengono aggiornate automaticamente ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati. Non è possibile modificare i controlli standard. Tuttavia, è possibile creare una copia modificabile di qualsiasi controllo standard.
Controllo personalizzato	Si tratta di un controllo creato in Audit Manager per soddisfare i requisiti di conformità specifici. È possibile creare un controllo personalizzato partendo da zero o creare una copia modificabile di un controllo standard esistente. Quando si crea un controllo personalizzato, è possibile definire elementi specifici evidence source che determinano da dove Audit Manager raccoglie le prove. Dopo aver creato un controllo personalizzato, è possibile modificare tale controllo o aggiungerlo a un framework personalizzato. È inoltre possibile creare una copia modificabile di qualsiasi controllo personalizzato.

Dominio di controllo

Puoi pensare a un dominio di controllo come a una categoria di controlli che non rientra in alcun standard di conformità. Un esempio di dominio di controllo è la protezione dei dati.

I controlli sono spesso raggruppati per dominio per semplici scopi organizzativi. Ogni dominio ha più obiettivi.

I raggruppamenti di domini di controllo sono una delle funzionalità più potenti del pannello di controllo di Gestione audit. Gestione audit evidenzia i controlli che nelle valutazioni presentano prove non conformi e li raggruppa per dominio di controllo. Ciò consente di concentrare gli sforzi di correzione su domini tematici specifici mentre ci si prepara per un audit.

Obiettivo di controllo

Un obiettivo di controllo descrive l'obiettivo dei controlli comuni che lo sottendono. Ogni obiettivo può avere più controlli comuni. Se questi controlli comuni vengono implementati con successo, ti aiuteranno a raggiungere l'obiettivo.

Ogni obiettivo di controllo rientra in un dominio di controllo. Ad esempio, il dominio di controllo della protezione dei dati potrebbe avere un obiettivo di controllo denominato Classificazione e gestione dei dati. Per supportare questo obiettivo di controllo, è possibile utilizzare un controllo comune denominato Controlli di accesso per monitorare e rilevare gli accessi non autorizzati alle risorse.

Controllo di base

Per informazioni, consulta control.

Controllo personalizzato

Per informazioni, consulta control.

Fonte gestita dal cliente

Una fonte gestita dal cliente è una fonte di prove definita dall'utente.

Quando crei un controllo personalizzato in Audit Manager, puoi utilizzare questa opzione per creare le tue fonti di dati individuali. Ciò offre la flessibilità necessaria per raccogliere prove automatizzate da una risorsa specifica dell'azienda, ad esempio una regola personalizzata AWS Config . Puoi utilizzare questa opzione anche se desideri aggiungere prove manuali al tuo controllo personalizzato.

Quando utilizzi fonti gestite dai clienti, sei responsabile della manutenzione di tutte le fonti di dati che crei.

Vedi anche:AWS managed source,evidence source.

D

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Origine dati

Audit Manager utilizza fonti di dati per raccogliere prove per un controllo. Un'origine dati ha le seguenti proprietà:

- Un tipo di origine dati definisce da quale tipo di origine dati Audit Manager raccoglie le prove.
  - Per le prove automatiche, il tipo può essere AWS Security HubAWS Config AWS CloudTrail, o chiamate AWS API.
  - Se carichi le tue prove, il tipo è Manuale.
  - L'API Audit Manager fa riferimento a un tipo di origine dati come SourceType.
- Una mappatura dell'origine dati è una parola chiave che indica da dove vengono raccolte le prove per un determinato tipo di origine dati.
  - Ad esempio, potrebbe essere il nome di un CloudTrail evento o il nome di una AWS Config regola.
  - L'API Audit Manager fa riferimento a una mappatura dell'origine dati come SourceKeyword.
- Il nome di un'origine dati indica l'associazione tra un tipo di origine dati e una mappatura.
  - Per i controlli standard, Audit Manager fornisce un nome predefinito.
  - Per i controlli personalizzati, puoi fornire il tuo nome.
  - API Gestione audit fa riferimento al nome di un'origine dati come sourceName.

Un singolo controllo può avere più tipi di origini dati e più mappature. Ad esempio, un controllo potrebbe raccogliere prove da una combinazione di tipi di fonti di dati (ad AWS Config esempio Security Hub). Un altro controllo potrebbe avere AWS Config come unico tipo di origine dati, con più AWS Config regole come mappature.

La tabella seguente elenca i tipi di origine dati automatizzati e mostra esempi di alcune mappature corrispondenti.

Tipo di origine dati	Descrizione	Esempio di mappatura
AWS Security Hub	Utilizza questo tipo di origine dati per acquisire un'istant anea dello stato di sicurezza delle tue risorse. Gestione audit utilizza il nome di un controllo Security Hub come parola chiave di mappatura ed esegue il report del risultato di tale controllo di sicurezza direttamente da Security Hub.	`EC2.1`
AWS Config	Utilizza questo tipo di origine dati per acquisire un'istant anea dello stato di sicurezza delle tue risorse. Audit Manager utilizza il nome di una AWS Config regola come parola chiave di mappatura e riporta il risultato del controllo di tale regola direttamente da AWS Config.	`SNS_ENCRYPTED_KMS`
AWS CloudTrail	Utilizza questo tipo di origine dati per tenere traccia di un'attività utente specifica necessaria per il tuo audit. Audit Manager utilizza il nome di un CloudTrail evento come parola chiave di mappatura e raccoglie l'attivit	`CreateAccessKey`

Tipo di origine dati	Descrizione	Esempio di mappatura
	à utente correlata dai registri. CloudTrail	
AWS Chiamate API	Utilizza questo tipo di origine dati per scattare un'istantanea della configura zione delle risorse tramite una chiamata API a una determinata Servizio AWS risorsa. Gestione audit utilizza il nome della chiamata API come parola chiave di mappatura e raccoglie la risposta API.	`kms_ListKeys`

Delegato

Un delegato è un AWS Audit Manager utente con autorizzazioni limitate. Generalmente, i delegati hanno competenze commerciali o tecniche specializzate. Ad esempio, queste competenze potrebbero riguardare le policy di conservazione dei dati, i piani di formazione, l'infrastruttura di rete o la gestione delle identità. I delegati aiutano i proprietari degli audit a esaminare le prove raccolte per i controlli che rientrano nella loro area di competenza. I delegati possono esaminare i set di controlli e le relative prove, aggiungere commenti, caricare prove aggiuntive e aggiornare lo stato di un controllo loro assegnato per la revisione.

I proprietari degli audit delegano specifici set di controlli ai delegati, non intere valutazioni. Di conseguenza, i delegati hanno un accesso limitato alle valutazioni. Per istruzioni su come delegare un set di controlli, consulta Delegazioni in AWS Audit Manager.

E

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Prove

Le prove sono registrazioni che contengono le informazioni necessarie per dimostrare la conformità ai requisiti di un controllo. Esempi di prove includono un'attività di modifica richiamata da un utente e un'istantanea della configurazione del sistema.

Esistono due tipi principali di prove in Gestione audit: prove automatiche e prove manuali.

Tipo di prova	Descrizione
Prove automatizzate	Queste sono le prove che Audit Manager raccoglie automaticamente. Sono incluse le seguenti tre categorie di prove automatiche: 1. Controllo di conformità: il risultato di un controllo di conformità viene acquisito da AWS Security Hub o da entrambi. AWS Config Esempi di controlli di conformità includono un risultato del controllo di sicurezza di Security Hub per un controllo PCI DSS e una valutazione delle AWS Config regole per un controllo HIPAA. Per ulteriori informazioni, consulta Regole di AWS Config supportato da AWS Audit Manager e AWS Security Hub controlli supportati da AWS Audit Manager. 2. Attività dell'utente: l'attività dell'utente che modifica la configurazione di una risorsa viene acquisita dai CloudTrail log nel momento in cui si verifica tale attività. Esempi di attività utente includono l'aggiornamento della tabella di routing, la modifica delle impostazioni di backup dell'istanza Amazon RDS e la modifica della policy di crittografia dei bucket S3. Per ulteriori informazioni, consulta AWS CloudTrail nomi di eventi supportati da AWS Audit Manager. 3. Dati di configurazione: l'istantanea della configurazione delle risorse viene acquisita direttamente da un Servizio AWS su base giornaliera, settimanale o mensile. Esempi di istantanee di configurazione includono un elenco di route per una tabella di routing VPC, un'impostazione di backup dell'istanza Amazon RDS e una policy di crittografia dei bucket S3.

Tipo di prova	Descrizione
	Per ulteriori informazioni, consulta AWS Chiamate API supportate da AWS Audit Manager.
Evidenza manuale	Questa è la prova che aggiungi tu stesso all'Audit Manager. Esistono tre modi per aggiungere le proprie prove: 1. Importazione di un file da Amazon S3 2. Caricamento di un file dal tuo browser 3. Inserimento di una risposta testuale a una domanda di valutazione del rischio Per ulteriori informazioni, consulta Aggiungere prove manuali in AWS Audit Manager.

La raccolta automatica delle prove inizia nel momento in cui viene creata una valutazione. Si tratta di un processo continuo e Gestione audit raccoglie le prove con frequenze diverse a seconda del tipo di prova e dell'origine dati sottostante. Per ulteriori informazioni, consulta Comprendere come AWS Audit Manager raccoglie le prove.

Per istruzioni su come esaminare le prove in una valutazione, consulta Revisione delle prove in AWS Audit Manager.

Fonte delle prove

Una fonte di prove definisce da dove un controllo raccoglie le prove. Può essere una singola fonte di dati o un raggruppamento predefinito di fonti di dati che si associa a un controllo comune o a un controllo principale.

Quando crei un controllo personalizzato, puoi raccogliere prove da fonti AWS gestite, fonti gestite dai clienti o entrambe.

> **Tip**
>
> Ti consigliamo di utilizzare fonti AWS gestite. Ogni volta che una fonte AWS gestita viene aggiornata, gli stessi aggiornamenti vengono applicati automaticamente a tutti i controlli personalizzati che utilizzano tali fonti. Ciò significa che i controlli personalizzati raccolgono

sempre prove in base alle definizioni più recenti di quella fonte di prove. Questo ti aiuta a garantire una conformità continua man mano che l'ambiente di conformità cloud cambia.

Vedi anche:AWS managed source,customer managed source.

Metodo di raccolta delle prove

Esistono due modi in cui un controllo può raccogliere le prove.

Metodo di raccolta delle prove	Descrizione
Automatizzato	I controlli automatici raccolgono automaticamente prove dalle fonti di AWS dati. Queste prove automatiche possono aiutare a dimostrare la conformità totale o parziale al controllo.
Manuale	I controlli manuali richiedono il caricamento di prove personali per dimostrare la conformità al controllo.

Note

È possibile allegare prove manuali a qualsiasi controllo automatico. In molti casi, è necessaria una combinazione di prove automatiche e manuali per dimostrare la piena conformità a un controllo. Sebbene Gestione audit sia in grado di fornire prove automatiche utili e pertinenti, alcune prove automatiche potrebbero dimostrare solo una conformità parziale. In questo caso, puoi integrare le prove automatiche fornite da Gestione audit con le tue prove.
Per esempio:

- AWS framework generativo per le migliori pratiche di intelligenza artificiale v2Contiene un controllo chiamato`Error analysis`. Questo controllo chiede di indicare le imprecisioni rilevate nell'utilizzo del modello. Richiede inoltre di condurre un'analisi approfondita degli errori per comprenderne le cause alla radice e intraprendere azioni correttive.
- Per supportare questo controllo, Audit Manager raccoglie prove automatiche che mostrano se gli CloudWatch allarmi sono abilitati per il Account AWS luogo in cui è in

corso la valutazione. È possibile utilizzare queste prove per dimostrare la conformità parziale al controllo, provando che gli allarmi e i controlli sono configurati correttamente.

- Per dimostrare la piena conformità, è possibile integrare le prove automatiche con prove manuali. Ad esempio, è possibile caricare una policy o una procedura che mostri il processo di analisi degli errori, le soglie per le escalation e il reporting nonché i risultati dell'analisi delle cause principali. È possibile utilizzare queste prove manuali per dimostrare che le policy stabilite sono state applicate e che sono state intraprese azioni correttive quando richiesto.

Per un esempio più dettagliato, consulta Controlli con origini dati miste.

Destinazione di esportazione

Una destinazione di esportazione è il bucket S3 predefinito in cui Gestione audit salva i file esportati da Evidence Finder. Per ulteriori informazioni, consulta Configurazione della destinazione di esportazione predefinita per Evidence Finder.

F

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Framework

Un framework Audit Manager struttura e automatizza le valutazioni per uno specifico standard o principio di governance del rischio. Questi framework includono una raccolta di controlli predefiniti o definiti dal cliente e consentono di mappare AWS le risorse in base ai requisiti di questi controlli.

Esistono due tipi di framework in Audit Manager.

Tipo di framework	Descrizione
Struttura standard	Si tratta di un framework predefinito basato sulle AWS migliori pratiche per vari standard e normative di conformità. È possibile utilizzare framework standard per facilitare la preparazione degli audit per uno specifico standard o regolamento di conformità, come PCI DSS o HIPAA.

Tipo di framework	Descrizione
Framework personalizzato	Si tratta di un framework personalizzato che definisci come utente Audit Manager. È possibile utilizzare framework personalizzati per facilitare la preparazione degli audit in base ai requisiti GRC specifici.

Per istruzioni su come creare e gestire i framework, consulta Utilizzo della libreria di framework per gestire i framework in AWS Audit Manager.

> **Note**
>
> AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e regolamenti di conformità. Tuttavia, non viene eseguita la valutazione della conformità. AWS Audit Manager Pertanto, le prove raccolte potrebbero non includere tutte le informazioni sull' AWS utilizzo necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Condivisione del framework

Puoi utilizzare la Condivisione di un framework personalizzato in AWS Audit Manager funzione per condividere rapidamente i tuoi framework personalizzati tra tutte le regioni. Account AWS Per condividere un framework personalizzato, è necessario creare una richiesta di condivisione. Il destinatario ha quindi 120 giorni per accettare o rifiutare la richiesta. Se il destinatario accetta, Gestione audit replica il framework personalizzato condiviso nella sua libreria di framework. Oltre a replicare il framework personalizzato, Gestione audit replica anche tutti i set di controlli e i controlli personalizzati contenuti in tale framework. I controlli personalizzati vengono aggiunti alla libreria di controlli del destinatario. Gestione audit non replica framework o controlli standard. Questo perché si tratta di risorse già disponibili per impostazione predefinita in ogni account e regione.

R

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Risorsa

Una risorsa è una risorsa fisica o informativa che viene valutata in un audit. Esempi di AWS risorse includono istanze Amazon EC2, istanze Amazon RDS, bucket Amazon S3 e sottoreti Amazon VPC.

Valutazione della risorsa

La valutazione della risorsa è il processo di valutazione di una singola risorsa. La valutazione si basa sul requisito di un controllo. Mentre una valutazione è attiva, Gestione audit valuta ogni singola risorsa nell'ambito della valutazione. La valutazione della risorsa esegue la seguente serie di attività:

1. Raccoglie prove tra cui configurazioni delle risorse, log di eventi e risultati
2. Traduce e mappa le prove ai controlli
3. Memorizza e tiene traccia del percorso delle prove per garantire l'integrità

Conformità della risorsa

La conformità della risorsa si riferisce allo stato di valutazione di una risorsa che è stata valutata durante la raccolta delle prove di controllo di conformità.

Audit Manager raccoglie prove di verifica della conformità per i controlli che utilizzano AWS Config Security Hub come tipo di origine dati. Durante la raccolta delle prove potrebbero essere valutate più risorse. Di conseguenza, una singola prova di controllo di conformità può includere una o più risorse.

Puoi utilizzare il filtro Conformità delle risorse in Evidence Finder per esplorare lo stato di conformità a livello di risorsa. Una volta completata la ricerca, puoi visualizzare in anteprima le risorse corrispondenti alla tua query di ricerca.

In Evidence Finder, ci sono tre possibili valori per la conformità delle risorse:

Valore	Descrizione
Non conforme	Si riferisce alle risorse con problemi di controllo della conformità. Ciò accade se Security Hub riporta un risultato Fail per la risorsa o se AWS Config riporta un risultato non conforme.
Conforme	Si riferisce a risorse che non presentano problemi di controllo della conformità.

Valore	Descrizione
	Ciò accade se Security Hub riporta un risultato Pass per la risorsa o se AWS Config riporta un risultato Conforme.
Inconcludente	Si riferisce a risorse per le quali un controllo di conformità non è disponibile o applicabile. Ciò accade se AWS Config o Security Hub è il tipo di origine dati sottostante, ma tali servizi non sono abilitati. Ciò accade anche se il tipo di origine dati sottostante non supporta i controlli di conformità (come prove manuali, chiamate AWS API o CloudTrail).

S

| B | | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Servizio in ambito

Audit Manager gestisce ciò Servizi AWS che rientra nell'ambito delle vostre valutazioni. Se disponi di una valutazione precedente, è possibile che in passato tu abbia specificato manualmente i servizi inclusi nell'ambito. Dopo il 4 giugno 2024, non è possibile specificare o modificare manualmente i servizi inclusi nell'ambito.

Un servizio rientrante è un servizio su Servizio AWS cui la valutazione raccoglie prove. Quando un servizio è incluso nell'ambito della valutazione, Audit Manager valuta le risorse del servizio. Esempi di risorse sono:

- Un'istanza di Amazon EC2
- Un bucket S3
- Un utente o ruolo IAM
- Una tabella DynamoDB
- Un componente di rete come un cloud privato virtuale (VPC) di Amazon, un gruppo di sicurezza o una tabella con la lista di controllo degli accessi (ACL) di rete

Ad esempio, se Amazon S3 è un servizio che rientra nell'ambito di applicazione, Audit Manager può raccogliere prove sui bucket S3. Le prove esatte raccolte sono determinate da un controllo. data source Ad esempio, se il tipo di origine dati è AWS Config e la mappatura dell'origine dati è

una AWS Config regola (ad esempios3-bucket-public-write-prohibited), Audit Manager raccoglie il risultato della valutazione di tale regola come prova.

> **Note**
>
> Tieni presente che un servizio compreso nell'ambito è diverso da un tipo di origine dati, che può anche essere una Servizio AWS o qualcos'altro. Per ulteriori informazioni, Qual è la differenza tra un servizio in ambito e un tipo di origine dati? consulta la sezione Risoluzione dei problemi di questa guida.

Controllo standard

Per informazioni, consulta control.

Comprendere come AWS Audit Manager raccogliere le prove

Ogni valutazione attiva raccoglie AWS Audit Manager automaticamente prove da una serie di fonti di dati. In ogni valutazione, definisci per quale Account AWS Audit Manager raccoglierà le prove e Audit Manager gestirà quali Servizi AWS rientrano nell'ambito. Ciascuno di questi servizi e account contiene più risorse che l'utente possiede e utilizza. La raccolta delle prove in Gestione audit implica la valutazione di ogni risorsa in ambito. Questa operazione viene definita valutazione della risorsa.

I passaggi seguenti descrivono come Gestione audit raccoglie le prove per ogni valutazione della risorsa:

1. Valutazione di una risorsa dall'origine dati

Per avviare la raccolta delle prove, Gestione audit valuta una risorsa in ambito da un'origine dati. A tale scopo, acquisisce un'istantanea della configurazione, un risultato del relativo controllo di conformità o l'attività dell'utente. Dopodiché esegue un'analisi per determinare quale sia il controllo supportato da questi dati. Il risultato della valutazione della risorsa viene quindi salvato e convertito in prova. Per ulteriori informazioni sui diversi tipi di prove, consulta la sezione relativa evidence ai AWS Audit Manager concetti e alla terminologia di questa guida.

2. Conversione dei risultati della valutazione in prova

Il risultato della valutazione delle risorse contiene sia i dati originali acquisiti da quella risorsa, sia i metadati che indicano il controllo supportato dai dati. Audit Manager converte i dati originali in un

formato adatto ai revisori. I dati e i metadati convertiti vengono quindi salvati come prove di Gestione audit prima di essere associati a un controllo.

3. Associazione delle prove al relativo controllo

Gestione audit legge i metadati delle prove. Quindi, allega le prove salvate a un controllo correlato all'interno della valutazione. La prova associata diventa visibile in Gestione audit. Questo completa il ciclo di valutazione di una risorsa.

> **Note**
>
> A seconda delle configurazioni di controllo, in alcuni casi è possibile associare la stessa prova a più controlli provenienti da più valutazioni Gestione audit. Quando la stessa prova è associata a più controlli, Gestione audit misura la valutazione della risorsa esattamente una volta. Questo perché la stessa prova viene raccolta esattamente una sola volta. Tuttavia, un controllo presente in una valutazione di Gestione audit può avere più prove provenienti da più origini dati.

Frequenza di raccolta delle prove

Il processo di raccolta delle prove è continuo e inizia nel momento in cui si crea una valutazione. Audit Manager raccoglie prove da più fonti di dati con frequenze diverse. Di conseguenza, non esiste una one-size-fits-all risposta alla frequenza con cui vengono raccolte le prove. La frequenza della raccolta delle prove si basa sul tipo di prova e sulla relativa origine dati, come descritto di seguito.

- Controlli di conformità: Audit Manager raccoglie questo tipo di prove da AWS Security Hub e AWS Config.
  - Per Security Hub, la raccolta delle prove segue la pianificazione dei controlli del Security Hub. Per ulteriori informazioni sulla pianificazione dei controlli di Security Hub, consulta Pianificazione per l'esecuzione dei controlli di sicurezza nella AWS Security Hub Guida per l'utente. Per ulteriori informazioni sui controlli di Security Hub supportati da Gestione audit, consulta AWS Security Hub controlli supportati da AWS Audit Manager.
  - Infatti AWS Config, la raccolta delle prove segue i fattori scatenanti definiti nelle tue AWS Config regole. Per ulteriori informazioni sui trigger delle regole AWS Config , consulta Tipi di trigger nella AWS Config Guida per l'utente. Per ulteriori informazioni su Regole di AWS Config ciò che è supportato da Audit Manager, vedereRegole di AWS Config supportato da AWS Audit Manager.

- Attività dell'utente: Audit Manager raccoglie questo tipo di prove AWS CloudTrail in modo continuo. La frequenza è continua perché l'attività dell'utente può avvenire in qualsiasi momento della giornata. Per ulteriori informazioni, consulta AWS CloudTrail nomi di eventi supportati da AWS Audit Manager.
- Dati di configurazione: Audit Manager raccoglie questo tipo di prove utilizzando una chiamata API di descrizione a un'altra Servizio AWS come Amazon EC2, Amazon S3 o IAM. È possibile scegliere quali azioni API chiamare. È inoltre possibile impostare una frequenza giornaliera, settimanale o mensile in Gestione audit. È possibile specificare questa frequenza quando si crea o si modifica un controllo nella libreria dei controlli. Per istruzioni su come modificare o creare un controllo, consulta Utilizzo della libreria di controlli per gestire i controlli in AWS Audit Manager. Per ulteriori informazioni sulle chiamate API supportate da Audit Manager, vedereAWS Chiamate API supportate da AWS Audit Manager.

Indipendentemente dalla frequenza di raccolta delle prove per l'origine dati, le nuove prove vengono raccolte automaticamente finché il controllo e la valutazione sono attivi.

Esempi di AWS Audit Manager controlli

Puoi consultare gli esempi in questa pagina per ulteriori informazioni su come funzionano i controlli in AWS Audit Manager.

In Audit Manager, i controlli possono raccogliere automaticamente prove da quattro tipi di fonti di dati:

1. AWS CloudTrail— Acquisisci l'attività degli utenti dai tuoi CloudTrail registri e importala come prova dell'attività dell'utente
2. AWS Security Hub— Raccogli i risultati da Security Hub e importali come prove di verifica della conformità
3. AWS Config— Raccogli le valutazioni delle regole AWS Config e le importa come prove di verifica della conformità
4. AWS Chiamate API: acquisisci un'istantanea della risorsa da una chiamata API e importala come prova dei dati di configurazione

Molti controlli raccolgono prove utilizzando raggruppamenti predefiniti di queste fonti di dati. Questi raggruppamenti di fonti di dati sono noti come AWS fonti gestite. Ogni fonte AWS gestita rappresenta un controllo comune o un controllo principale. Questo ti offre un modo efficiente per mappare i

requisiti di conformità a un gruppo pertinente di fonti di dati, convalidate e gestite da valutatori certificati del settore in. AWS In alternativa, puoi utilizzare i quattro tipi di fonti di dati precedenti per definire le tue fonti di dati. Ciò offre la flessibilità necessaria per caricare prove manuali o raccogliere prove automatizzate da una risorsa specifica dell'azienda, ad esempio una regola personalizzata AWS Config .

Gli esempi in questa pagina mostrano come i controlli raccolgono prove da ciascuno dei singoli tipi di fonti di dati. Descrivono l'aspetto di un controllo, il modo in cui l'Audit Manager raccoglie le prove dalla fonte dei dati e i passaggi successivi che è possibile intraprendere per dimostrare la conformità.

> **Tip**
>
> Ti consigliamo di abilitare AWS Config e Security Hub per un'esperienza ottimale in Audit Manager. Quando abiliti questi servizi, Audit Manager può utilizzare i risultati del Security Hub e Regole di AWS Config generare prove automatiche.
>
> - Dopo aver abilitato AWS Security Hub, assicurati di abilitare anche tutti gli standard di sicurezza e di attivare l'impostazione dei risultati del controllo consolidato. Questo passaggio garantisce che Gestione audit possa importare i risultati per tutti gli standard di conformità supportati.
> - Dopo averlo abilitato AWS Config, assicurati di abilitare anche quello pertinente Regole di AWS Config o di implementare un pacchetto di conformità per lo standard di conformità correlato al tuo audit. Questo passaggio garantisce che Audit Manager possa importare i risultati per tutti i file supportati Regole di AWS Config che hai abilitato.

Sono disponibili esempi per ciascuno dei seguenti tipi di controlli:

Argomenti

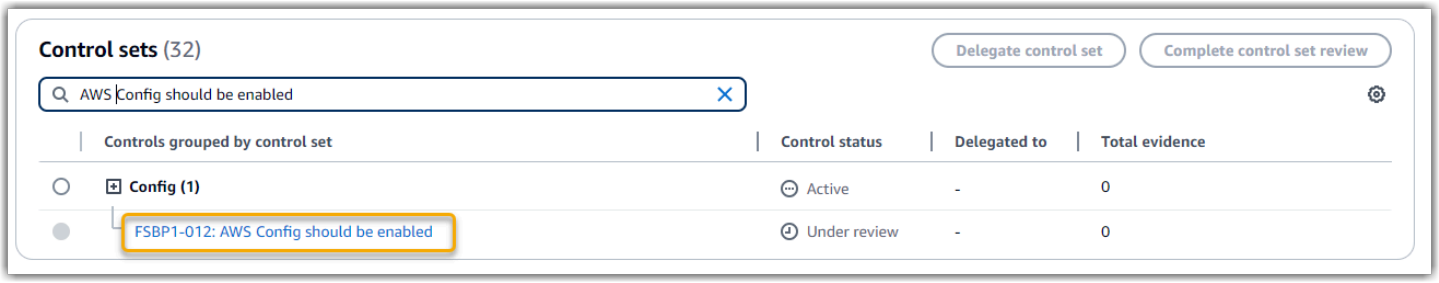
Controlli automatici che vengono utilizzati AWS Security Hub come tipo di origine dati

Questo esempio mostra un controllo che utilizza AWS Security Hub come tipo di origine dati. Si tratta di un controllo standard preso dal framework AWS Foundational Security Best Practices (FSBP). Audit Manager utilizza questo controllo per generare prove che possono contribuire a rendere AWS l'ambiente in linea con i requisiti FSBP.

Esempio di dettagli di controllo

- Nome del controllo: `FSBP1-012: AWS Config should be enabled`
- Set di controllo:. `Config` Si tratta di un raggruppamento specifico del framework di controlli FSBP relativi alla gestione della configurazione.
- Fonte di prove: fonti di dati individuali
- Tipo di fonte dati: AWS Security Hub
- Tipo di prova: controllo di conformità

Nell'esempio seguente, questo controllo si trova all'interno di una valutazione di Gestione audit creata dal framework FSBP.



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

Questo controllo richiede che AWS Config sia abilitato in tutti i Regioni AWS luoghi in cui si utilizza Security Hub. Gestione audit può utilizzare questo controllo per verificare se le tue policy IAM siano troppo ampie per soddisfare i requisiti FSBP. Più specificamente, può verificare se le policy

IAM gestite dai tuoi clienti dispongano dell'accesso da amministratore, che include la seguente dichiarazione con carattere jolly: `"Effect": "Allow"` con `"Action": "*"` su `"Resource": "*"`.

In che modo Gestione audit raccoglie le prove per questo controllo

Gestione audit adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Gestione audit valuta le risorse in ambito. A tale scopo, utilizza l'origine dati specificata nelle impostazioni di controllo. In questo esempio, le policy IAM sono la risorsa e Security Hub e AWS Config sono il tipo di origine dati. Audit Manager cerca il risultato di un controllo specifico del Security Hub ([IAM.1]), che a sua volta utilizza una AWS Config regola per valutare le policy IAM (iam-policy-no-statements- with-admin-access).
2. Il risultato della valutazione della risorsa viene quindi salvato e convertito in una prova utilizzabile dai revisori. Gestione audit genera una prova di controllo di conformità per i controlli che utilizzano Security Hub come tipo di origine dati. La prova contiene il risultato del controllo di conformità riportato direttamente da Security Hub.
3. Gestione audit allega le prove salvate al controllo nella tua valutazione denominata `FSBP1-012: AWS Config should be enabled`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Dopo aver allegato le prove al controllo, tu o un delegato di tua scelta potete esaminarle per vedere se è necessaria una correzione.

In questo esempio, Gestione audit potrebbe visualizzare una regola Fail di Security Hub. Ciò può accadere se le policy IAM contengono caratteri jolly (*) e sono troppo ampie per soddisfare il controllo. In questo caso, puoi aggiornare le tue policy IAM in modo che non consentano privilegi amministrativi completi. Per farlo, puoi determinare quali attività gli utenti debbano eseguire e creare quindi policy che permettano agli utenti di eseguire solo tali attività. Questa azione correttiva aiuta a rendere l' AWS ambiente in linea con i requisiti FSBP.

Quando le tue policy IAM sono in linea con il controllo, contrassegna il controllo come Revisionato e aggiungi le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

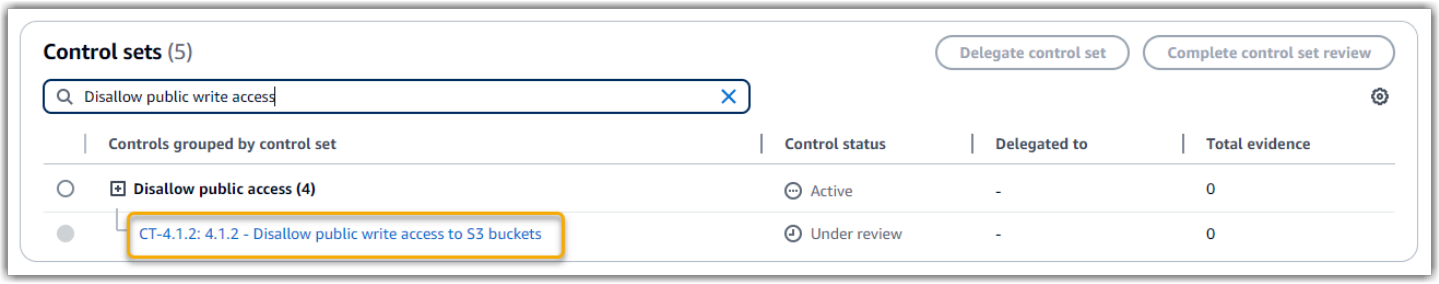
Controlli automatici che vengono utilizzati AWS Config come tipo di origine dati

Questo esempio mostra un controllo che utilizza AWS Config come tipo di origine dati. Questo è un controllo standard preso dal AWS Control Tower framework Guardrail. Audit Manager utilizza questo controllo per generare prove che aiutano a allineare AWS l'ambiente a AWS Control Tower Guardrails.

Esempio di dettagli di controllo

- Nome del controllo: `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- Set di controlli: questo controllo appartiene al set di controlli `Disallow public access`. Si tratta di un raggruppamento di controlli relativi alla gestione degli accessi.
- Fonte di prove: fonti di dati individuali
- Tipo di fonte dati: AWS Config
- Tipo di prova: controllo di conformità

Nell'esempio seguente, questo controllo si trova all'interno di una valutazione Audit Manager creata dal framework AWS Control Tower Guardrails.



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

Audit Manager può utilizzare questo controllo per verificare se i livelli di accesso delle policy dei bucket S3 sono troppo indulgenti per soddisfare i requisiti. AWS Control Tower Più specificamente,

può controllare le impostazioni di Blocco dell'accesso pubblico, le policy dei bucket e le liste di controllo degli accessi del bucket (ACL) per confermare che i bucket non consentano l'accesso pubblico in scrittura.

In che modo Gestione audit raccoglie le prove per questo controllo

Gestione audit adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Gestione audit valuta le risorse in ambito utilizzando l'origine dati specificata nelle impostazioni di controllo. In questo caso, i bucket S3 sono la risorsa e AWS Config è il tipo di origine dati. Audit Manager cerca il risultato di una AWS Config regola specifica (s3- bucket-public-write-prohibited) per valutare le impostazioni, i criteri e l'ACL di ciascuno dei bucket S3 che rientrano nell'ambito della valutazione.
2. Il risultato della valutazione della risorsa viene quindi salvato e convertito in una prova utilizzabile dai revisori. Audit Manager genera prove di verifica della conformità per i controlli utilizzati AWS Config come tipo di origine dati. Questa evidenza contiene il risultato del controllo di conformità riportato direttamente da AWS Config.
3. Gestione audit allega le prove salvate al controllo nella tua valutazione denominata `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Dopo aver allegato le prove al controllo, tu o un delegato di tua scelta potete esaminarle per vedere se è necessaria una correzione.

In questo esempio, Audit Manager potrebbe visualizzare una regola in base alla quale si AWS Config afferma che un bucket S3 non è conforme. Ciò potrebbe accadere se uno dei bucket S3 avesse un'impostazione Blocca accesso pubblico che non limita le policy pubbliche e la policy in uso consente l'accesso pubblico in scrittura. Per rimediare a questo problema, è possibile aggiornare l'impostazione Blocca accesso pubblico per limitare le policy pubbliche. In alternativa, è possibile utilizzare una policy bucket diversa che non consenta l'accesso pubblico in scrittura. Questa azione correttiva aiuta a rendere l'ambiente in linea con i requisiti. AWS AWS Control Tower

Quando si ritiene che i livelli di accesso al bucket S3 siano in linea con il controllo, è possibile contrassegnare il controllo come Rivisto e aggiungere le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

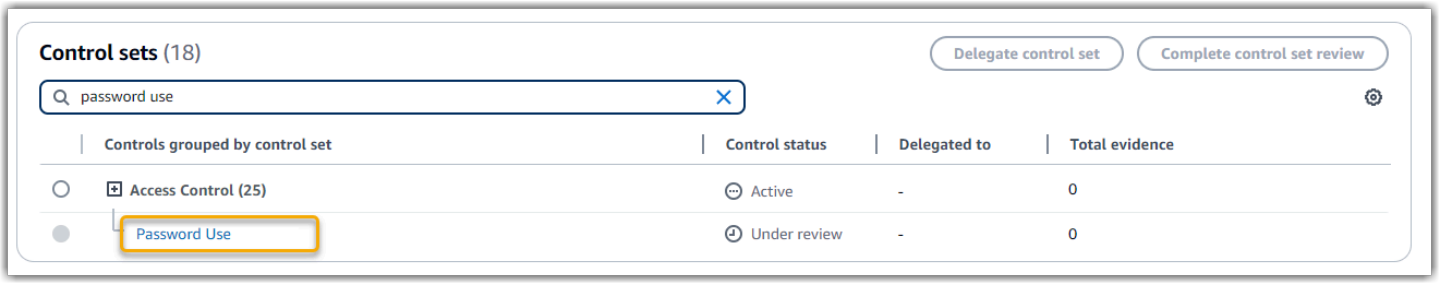
Controlli automatici che utilizzano le chiamate AWS API come tipo di origine dati

Questo esempio mostra un controllo personalizzato che utilizza le chiamate AWS API come tipo di origine dati. Audit Manager utilizza questo controllo per generare prove che possono contribuire a rendere AWS l'ambiente in linea con i requisiti specifici.

Esempio di dettagli di controllo

- Nome del controllo: `Password Use`
- Set di controlli: questo controllo appartiene al set di controlli chiamato `Access Control`. Si tratta di un raggruppamento di controlli relativi alla gestione delle identità e degli accessi.
- Fonte di prove: fonte di dati individuale
- Tipo di origine dati: chiamate AWS API
- Tipo di prova: dati di configurazione

Nell'esempio seguente, questo controllo si trova all'interno di una valutazione di Gestione audit creata da un framework personalizzato.



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

Gestione audit può utilizzare questo controllo personalizzato per contribuire a garantire l'esistenza di un numero sufficiente di policy di controllo degli accessi. Questo controllo richiede l'adozione di buone pratiche di sicurezza nella selezione e nell'uso delle password. Gestione audit può contribuire alla convalida di questo dato recuperando un elenco di tutte le policy sulle password per i principi IAM che rientrano nell'ambito della valutazione.

In che modo Gestione audit raccoglie le prove per questo controllo

Gestione audit adotta le seguenti misure per raccogliere prove per questo controllo personalizzato:

1. Per ogni controllo, Gestione audit valuta le risorse in ambito utilizzando l'origine dati specificata nelle impostazioni di controllo. In questo caso, i principali IAM sono le risorse e le chiamate AWS API sono il tipo di origine dati. Audit Manager cerca il risultato di una chiamata API IAM specifica (GetAccountPasswordPolicy). Quindi restituisce le policy relative alle password per gli Account AWS che rientrano nell'ambito della valutazione.
2. Il risultato della valutazione della risorsa viene quindi salvato e convertito in una prova utilizzabile dai revisori. Gestione audit genera le prove dei dati di configurazione per i controlli che utilizzano le chiamate API come origine dati. La prova contiene i dati originali acquisiti dalle risposte API e metadati aggiuntivi che indicano il controllo supportato dai dati.
3. Gestione audit allega le prove salvate al controllo personalizzato nella tua valutazione denominata `Password Use`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Dopo aver allegato le prove al controllo, tu o un delegato di tua scelta potete esaminarle per vedere se è sufficiente o se è necessaria una correzione.

In questo esempio, è possibile esaminare le prove per vedere le risposte della chiamata API. La GetAccountPasswordPolicyrisposta descrive i requisiti di complessità e i periodi di rotazione obbligatori per le password degli utenti nel tuo account. Puoi utilizzare questa risposta API come prova per dimostrare che disponi di politiche di controllo degli accessi tramite password sufficienti per quelle Account AWS che rientrano nell'ambito della tua valutazione. Se lo desideri, puoi anche fornire ulteriori commenti su queste policy aggiungendo un commento al controllo.

Quando ritieni che le policy sulle password dei principi IAM siano in linea con il controllo personalizzato, puoi contrassegnare il controllo come Rivisto e aggiungere le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

Controlli automatici che vengono utilizzati AWS CloudTrail come tipo di origine dati

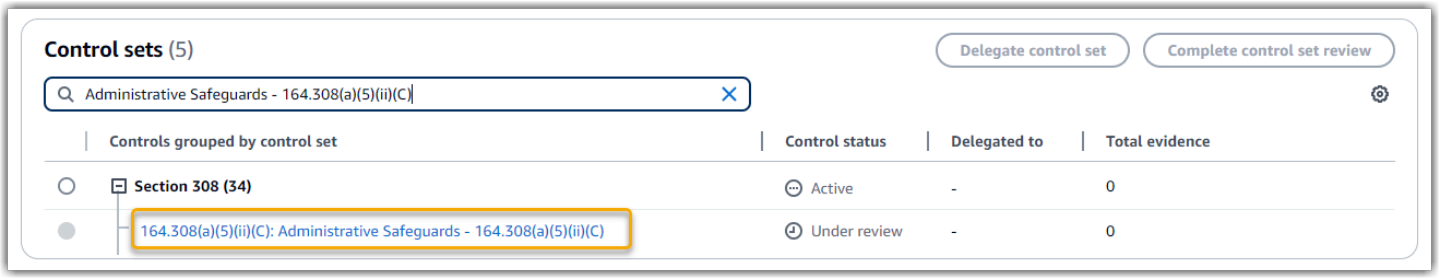
Questo esempio mostra un controllo che utilizza AWS CloudTrail come tipo di origine dati. Si tratta di un controllo standard tratto dal framework HIPAA Security Rule 2003. Gestione audit utilizza questo

controllo per generare prove che possono contribuire a rendere AWS l'ambiente in linea con i requisiti HIPAA.

Esempio di dettagli di controllo

- Nome del controllo: `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- Set di controlli: questo controllo appartiene al set di controlli chiamato `Section 308`. Si tratta di un raggruppamento specifico del framework di controlli HIPAA relativi alle garanzie amministrative.
- Fonte delle prove: fonte gestita (controlli di base) AWS
- Tipo di fonte di dati sottostante: AWS CloudTrail
- Tipo di prova: attività dell'utente

Ecco il controllo mostrato all'interno di una valutazione di Gestione audit creata dal framework HIPAA:



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

Questo controllo richiede l'adozione di procedure di monitoraggio per rilevare accessi non autorizzati. Un esempio di accesso non autorizzato si verifica quando qualcuno accede alla console senza abilitare l'autenticazione a più fattori (MFA). Audit Manager ti aiuta a convalidare questo controllo dimostrando che hai configurato Amazon per monitorare le richieste di accesso CloudWatch alla console di gestione in cui l'MFA non è abilitata.

In che modo Gestione audit raccoglie le prove per questo controllo

Gestione audit adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager valuta le risorse pertinenti utilizzando le fonti di evidenza specificate nelle impostazioni di controllo. In questo caso, il controllo utilizza diversi controlli di base come fonti di prova.

   Ogni controllo principale è un raggruppamento gestito di singole fonti di dati. Nel nostro esempio, uno di questi controlli principali (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) viene utilizzato CloudTrail come fonte di dati. CloudTrail è il tipo di origine dati e gli CloudWatch allarmi Amazon sono la risorsa che viene valutata.

   Audit Manager esamina CloudTrail i registri, utilizzando la `monitoring_EnableAlarmActions` parola chiave per trovare le azioni di attivazione degli CloudWatch allarmi registrate da. CloudTrail Quindi restituisce un log degli eventi rilevanti che rientrano nell'ambito della valutazione.
2. Il risultato della valutazione della risorsa viene quindi salvato e convertito in una prova utilizzabile dai revisori. Audit Manager genera prove dell'attività dell'utente per i controlli utilizzati CloudTrail come tipo di origine dati. Queste prove contengono i dati originali acquisiti da Amazon CloudWatch e metadati aggiuntivi che indicano il controllo supportato dai dati.
3. Gestione audit allega le prove salvate al controllo nella tua valutazione denominata `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Dopo aver allegato le prove al controllo, tu o un delegato di tua scelta potete esaminarle per vedere se è necessaria una correzione.

In questo esempio, puoi esaminare le prove per vedere gli eventi di attivazione degli allarmi registrati da. CloudTrail Puoi utilizzare questo registro come prova per dimostrare che disponi di procedure di monitoraggio sufficienti per rilevare quando gli accessi alla console avvengono senza l'MFA abilitata. Se lo desideri, puoi anche fornire ulteriori commenti su queste policy aggiungendo un commento al controllo. Ad esempio, se il registro mostra più accessi senza MFA, puoi aggiungere un commento che descrive come hai risolto il problema. Il monitoraggio regolare degli accessi alla console consente di prevenire i problemi di sicurezza che potrebbero derivare da discrepanze e tentativi di accesso inappropriati. A sua volta, questa best practice aiuta a rendere l' AWS ambiente in linea con i requisiti HIPAA.

Quando si ritiene che la procedura di monitoraggio sia in linea con il controllo, è possibile contrassegnare il controllo come Rivisto e aggiungere le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

Controlli manuali

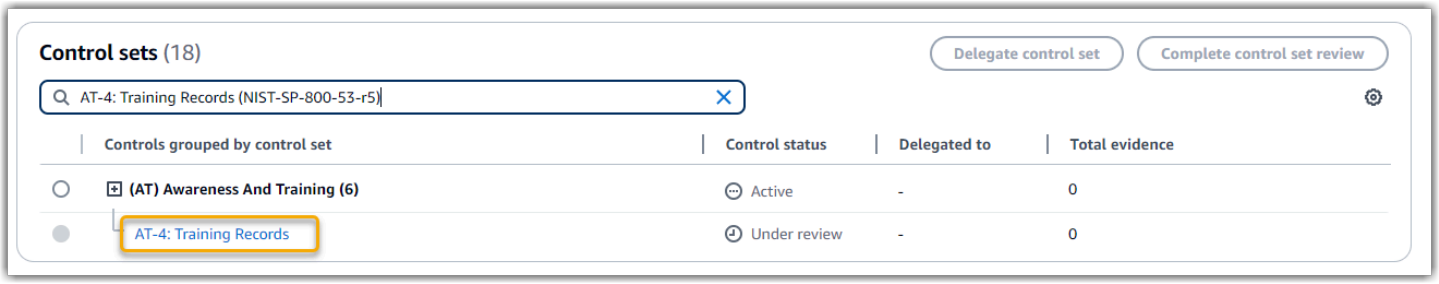
Alcuni controlli non supportano la raccolta automatica delle prove. Tra questi vi sono i controlli che si basano sulla fornitura di registrazioni e firme fisiche, oltre a osservazioni, interviste e altri eventi che non vengono generati nel cloud. In questi casi, è possibile caricare manualmente le prove per dimostrare che si stanno soddisfacendo i requisiti del controllo.

L'esempio mostra un controllo manuale per il quale Gestione audit non raccoglie prove automatiche. Si tratta di un controllo standard preso dal framework NIST 800-53 (Rev. 5). È possibile utilizzare Gestione audit per caricare e memorizzare le prove che dimostrano la conformità per questo controllo.

Esempio di dettagli di controllo

- Nome del controllo: `AT-4: Training Records`
- Set di controllo:`(AT) Awareness and training`. Si tratta di un raggruppamento specifico del framework di controlli NIST relativi alla formazione.
- Fonte di prove: fonti di dati
- Tipo di fonte di dati sottostante: manuale
- Tipo di prova: manuale

Ecco il controllo mostrato all'interno di una valutazione di Gestione audit creata dal framework NIST 800-53 (Rev. 5) Low-Moderate-High:



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

È possibile utilizzare questo controllo per garantire che il personale riceva il livello appropriato di formazione in materia di sicurezza e privacy. In particolare, puoi dimostrare di aver svolto attività di formazione documentate sulla sicurezza e sulla privacy per tutto il personale, in base al ruolo ricoperto. Puoi anche dimostrare che i registri di formazione vengono conservati per ogni individuo.

Come caricare manualmente le prove per questo controllo

Per caricare prove manuali che integrano le prove automatiche, vedi Caricamento delle prove manuali in. AWS Audit Manager Gestione audit allega le prove caricate al controllo nella valutazione denominata `AT-4: Training Records`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Se si dispone di documentazione che supporta questo controllo, è possibile caricarla come prova manuale. Ad esempio, puoi caricare la copia più recente dei materiali di formazione obbligatori basati sui ruoli che il reparto Risorse umane fornisce ai dipendenti.

Analogamente ai controlli automatici, è possibile delegare i controlli manuali alle parti interessate che possono aiutare a esaminare le prove (o, in questo caso, a fornirle). Ad esempio, esaminando questo controllo, potresti renderti conto di soddisfarne solo parzialmente i requisiti. Questo potrebbe accadere se non disponi di una copia del tracciamento delle presenze per i corsi di formazione in presenza. Potresti delegare il controllo a uno stakeholder delle risorse umane, che può quindi caricare un elenco del personale che ha partecipato alla formazione.

Quando ritieni che la procedura di monitoraggio sia in linea con il controllo, puoi contrassegnare il controllo come Rivisto e aggiungere le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

Controlli con tipi di origini dati misti (automatici e manuali)

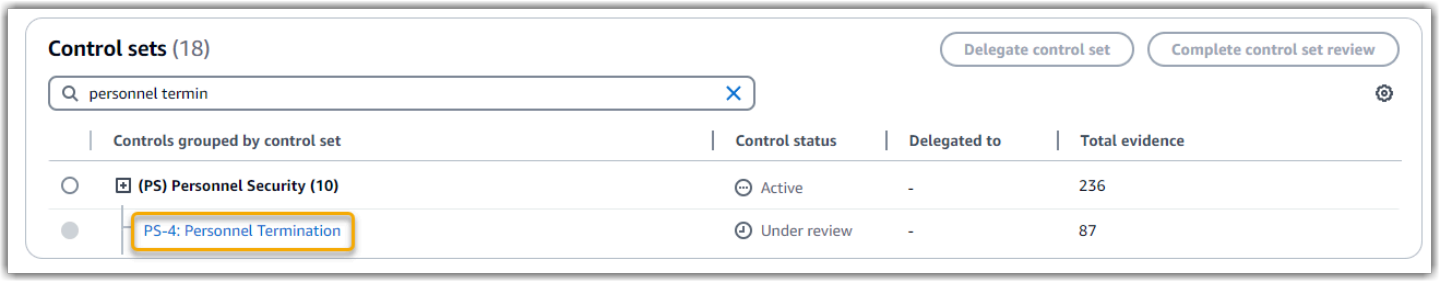
In molti casi, è necessaria una combinazione di prove automatiche e manuali per soddisfare un controllo. Sebbene Gestione audit sia in grado di fornire prove automatiche pertinenti al controllo, potrebbe essere necessario integrare questi dati con prove manuali che l'utente identifica e carica personalmente.

Questo esempio mostra un controllo che utilizza una combinazione di prove manuali e prove automatiche. Si tratta di un controllo standard preso dal framework NIST 800-53 (Rev. 5). Gestione audit utilizza questo controllo per generare prove che possono contribuire ad allineare l'ambiente AWS con i requisiti NIST.

Esempio di dettagli di controllo

- Nome del controllo: `Personnel Termination`
- Set di controllo:`(PS) Personnel Security (10)`. Si tratta di un raggruppamento specifico del framework di controlli NIST che si riferiscono alle persone che eseguono la manutenzione hardware o software sui sistemi organizzativi.
- Fonte delle prove: fonti di dati AWS gestite (controlli di base) e fonti di dati individuali (manuale)
- Tipo di origine dati sottostante: chiamate AWS API, AWS CloudTrail, AWS Config, Manuale
- Tipo di prova: dati di configurazione, attività dell'utente, controllo di conformità, prove manuali)

Ecco il controllo mostrato all'interno di una valutazione di Gestione audit creata dal framework NIST 800-53 (Rev. 5):



La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo. Da qui, puoi delegare il set di controlli alla revisione o completare tu stesso la revisione. Scegliendo il nome del controllo si apre una pagina di dettaglio con ulteriori informazioni, incluse le prove relative al controllo.

A cosa serve questo controllo

Puoi utilizzare questo controllo per confermare che stai proteggendo le informazioni organizzative in caso di licenziamento di un dipendente. In particolare, puoi dimostrare di aver disabilitato l'accesso al sistema e di aver revocato le credenziali dell'individuo. Inoltre, potete dimostrare che tutte le persone licenziate hanno partecipato a un colloquio di uscita che includeva una discussione sui protocolli di sicurezza pertinenti per la vostra organizzazione.

In che modo Gestione audit raccoglie le prove per questo controllo

Gestione audit adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager valuta le risorse pertinenti utilizzando le fonti di evidenza specificate nelle impostazioni di controllo.

In questo caso, il controllo utilizza diversi controlli di base come fonti di prova. A sua volta, ciascuno di questi controlli principali raccoglie prove pertinenti da singole fonti di dati (chiamate AWS API e AWS Config). AWS CloudTrail Audit Manager utilizza questi tipi di fonti di dati per valutare le risorse IAM (come gruppi, chiavi e policy) rispetto alle chiamate, CloudTrail agli eventi e AWS Config alle regole API pertinenti.

2. Il risultato della valutazione della risorsa viene quindi salvato e convertito in una prova utilizzabile dai revisori. Queste prove contengono i dati originali acquisiti da ciascuna fonte di dati e metadati aggiuntivi che indicano il controllo supportato dai dati.
3. Gestione audit allega le prove salvate al controllo nella tua valutazione denominata `Personnel Termination`.

Come caricare manualmente le prove per questo controllo

Per caricare prove manuali che integrano le prove automatiche, vedi Caricamento di prove manuali in. AWS Audit Manager Gestione audit allega le prove caricate al controllo nella valutazione denominata `Personnel Termination`.

Come utilizzare Gestione audit per dimostrare la conformità a questo controllo

Dopo aver allegato le prove al controllo, tu o un delegato di tua scelta potete esaminarle per vedere se è sufficiente o se è necessaria una correzione. Ad esempio, esaminando questo controllo, potresti renderti conto di soddisfarne solo parzialmente i requisiti. Questo potrebbe accadere se hai la prova che l'accesso è stato revocato, ma non hai una copia dei colloqui di uscita. Potresti delegare il controllo a uno stakeholder delle risorse umane, che può quindi caricare una copia dei documenti del colloquio di uscita. Oppure, se nessun dipendente è stato licenziato durante il periodo di audit, puoi lasciare un commento che spieghi perché al controllo non è allegato alcun documento firmato.

Quando si ritiene che la procedura di monitoraggio sia in linea con il controllo, è possibile contrassegnare il controllo come Rivisto e aggiungere le prove al report di valutazione. Puoi quindi condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

Integrazioni con prodotti correlati Servizi AWS

AWS Audit Manager si integra con più Servizi AWS strumenti per raccogliere automaticamente prove da includere nei report di valutazione.

AWS Security Hub

AWS Security Hub monitora l'ambiente utilizzando controlli di sicurezza automatizzati basati sulle AWS migliori pratiche e sugli standard del settore. Gestione audit acquisisce istantanee del livello di sicurezza delle risorse riportando i risultati dei controlli di sicurezza direttamente da Security Hub. Per ulteriori informazioni su Security Hub, vedi Cos'è AWS Security Hub? nella Guida AWS Security Hub per l'utente.

AWS CloudTrail

AWS CloudTrail ti aiuta a monitorare le chiamate effettuate alle AWS risorse del tuo account. Queste includono le chiamate effettuate dalla Console di AWS gestione, dalla AWS CLI e altro. Servizi AWS Audit Manager raccoglie CloudTrail direttamente i dati di registro e converte i registri elaborati in prove dell'attività dell'utente. Per ulteriori informazioni su CloudTrail, vedi Cos'è? AWS CloudTrail nella Guida AWS CloudTrail per l'utente.

AWS Config

AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo Account AWS. Questo include informazioni su come le risorse sono collegate tra loro e su come sono state configurate in passato. Audit Manager acquisisce istantanee del vostro stato di sicurezza delle risorse riportando i risultati direttamente da. AWS ConfigPer ulteriori informazioni su AWS Config, consulta What is? AWS Config nella Guida AWS Config per l'utente.

AWS License Manager

AWS License Manager semplifica il processo di trasferimento delle licenze dei fornitori di software sul cloud. Man mano che costruisci un'infrastruttura cloud AWS, puoi risparmiare sui costi riadattando l'inventario delle licenze esistente per utilizzarlo con le risorse cloud. Gestione audit fornisce un framework License Manager per assistere nella preparazione dell'audit. Il framework è integrato con License Manager per aggregare le informazioni sull'utilizzo delle licenze in base a regole di licenza definite dal cliente. Per ulteriori informazioni su License Manager, consulta What is AWS License Manager? nella Guida AWS License Manager per l'utente.

AWS Control Tower

AWS Control Tower impone barriere preventive e investigative per l'infrastruttura cloud. Audit Manager fornisce un framework AWS Control Tower Guardrails per assistervi nella preparazione dell'audit. Questo framework contiene tutte le AWS Config regole basate sui guardrails di. AWS Control Tower Per ulteriori informazioni su AWS Control Tower, vedi What is? AWS Control Tower nella Guida AWS Control Tower per l'utente.

AWS Artifact

AWS Artifact è un portale self-service per il recupero degli artefatti di audit che fornisce accesso su richiesta alla documentazione di conformità e alle certificazioni per l'infrastruttura. AWS AWS Artifact offre prove per dimostrare che l'infrastruttura Cloud soddisfa i requisiti di conformità AWS . Al contrario, ti AWS Audit Manager aiuta a raccogliere, esaminare e gestire le prove per dimostrare che l'utilizzo di Servizi AWS è conforme. Per ulteriori informazioni su AWS Artifact, consulta Cos'è AWS Artifact? nella Guida AWS Artifact per l'utente. È possibile scaricare un elenco di AWS report in AWS Management Console.

Amazon EventBridge

Amazon ti EventBridge aiuta ad automatizzare Servizi AWS e rispondere automaticamente a eventi di sistema come problemi di disponibilità delle applicazioni o modifiche delle risorse. È possibile utilizzare EventBridge le regole per rilevare e reagire agli eventi di Audit Manager. In base alle regole create, EventBridge richiama una o più azioni mirate quando un evento corrisponde ai valori specificati in una regola. A seconda del tipo di evento, potresti voler inviare notifiche, acquisire informazioni sull'evento, intraprendere un'azione correttiva, avviare eventi o eseguire altre operazioni. Per ulteriori informazioni, consulta Monitoraggio AWS Audit Manager con Amazon EventBridge.

Per un elenco dei programmi Servizi AWS di conformità specifici, vedere Servizi AWS Ambito di applicazione per programma di conformità. Per informazioni generali, consulta AWS Programmi di compliance.

Integrazioni con prodotti GRC di terze parti

AWS Audit Manager supporta le integrazioni con i prodotti GRC dei partner terzi elencati in questa pagina.

Se la tua azienda utilizza un modello di cloud ibrido o un modello multicloud, è probabile che utilizzi un prodotto GRC per gestire le prove provenienti da tali ambienti. Quando il prodotto è integrato con Audit Manager, puoi raccogliere prove sul tuo AWS utilizzo direttamente nel tuo ambiente GRC. Ciò semplifica il modo in cui gestite la conformità fornendoti un luogo centralizzato per esaminare e correggere le prove mentre ti prepari per gli audit.

Leggi questa pagina per una panoramica dei prodotti GRC di terze parti in grado di acquisire prove da Gestione audit. È inoltre possibile vedere un riferimento delle azioni API di Gestione audit che si possono eseguire direttamente all'interno di tali prodotti.

Argomenti

- Prodotti partner GRC di terze parti che si integrano con Gestione audit

Comprensione del funzionamento delle integrazioni di terze parti con Gestione audit

I partner GRC possono utilizzare le API pubbliche di Gestione audit per integrare i loro prodotti con Gestione audit. Con questa integrazione, è possibile mappare i controlli aziendali nel proprio ambiente GRC ai controlli comuni forniti da Audit Manager.

> **Tip**
>
> È possibile mappare i controlli aziendali su qualsiasi tipo di controllo Audit Manager. Tuttavia, ti consigliamo di utilizzare controlli comuni. Quando esegui il mapping su un controllo comune che rappresenta il tuo obiettivo, Audit Manager raccoglie prove da un gruppo predefinito di fonti di dati gestite da. AWS Ciò significa che non devi essere un AWS esperto per sapere quali fonti di dati raccolgono le prove pertinenti per il tuo obiettivo.

Dopo aver completato questo esercizio di mappatura dei controlli una tantum, puoi creare valutazioni Gestione audit direttamente nel prodotto GRC. Questa azione avvia la raccolta di prove sull' AWS utilizzo da parte tua. Potrai quindi visualizzare queste AWS prove insieme alle altre prove raccolte dal tuo ambiente ibrido, il tutto all'interno dello stesso contesto dei controlli aziendali.

Quando si utilizza un'integrazione Gestione audit con un prodotto GRC di terze parti, occorre tenere presenti i seguenti punti:

- Le integrazioni sono disponibili per tutte le Regioni AWS in cui è supportato Gestione audit.
- Tutte le risorse Gestione audit create nel prodotto partner GRC si riflettono anche in Gestione audit.
- Sei soggetto a AWS Audit Manager prezzi aggiuntivi oltre a quelli del prodotto GRC di terze parti.
- Le prove raccolte da Gestione audit sono immutabili. Le prove vengono presentate esattamente nello stesso modo nei prodotti GRC di terze parti come nella console di Gestione audit. Tuttavia, se utilizzi un'integrazione di terze parti, potresti avere la possibilità di migliorare le prove fornendo un contesto aggiuntivo nei tuoi report.
- Le stesse quote che si applicano ad Gestione audit si applicano anche all'interno del prodotto GRC di terze parti. Ad esempio, ogni Account AWS può avere fino a 100 valutazioni Gestione

audit attive. Questa quota a livello di account si applica indipendentemente dal fatto che le valutazioni siano state create nella console di Gestione audit o nel prodotto GRC di terze parti. La maggior parte delle quote di Audit Manager, ma non tutte, sono elencate nel AWS Audit Manager namespace nella console Service Quotas. Per sapere come richiedere un aumento delle quote, consulta Gestione delle proprie quote di Gestione audit.

Se disponi di una soluzione di conformità e sei interessato a integrarla con Gestione audit, invia un'e-mail a `auditmanager-partners@amazon.com`.

Prodotti partner GRC di terze parti che si integrano con Gestione audit

I seguenti prodotti GRC di terze parti possono acquisire prove da Gestione audit.

MetricStream

Per utilizzare questa integrazione, contatta l'indirizzo MetricStreamper l'accesso e l'acquisto del software GRC. MetricStream

Basata sulla MetricStream piattaforma, la soluzione MetricStream Enterprise GRC consente un approccio completo e collaborativo alle attività e ai processi GRC a livello aziendale. Inserendo le prove da Audit Manager in MetricStream, puoi identificare in modo proattivo le prove di non conformità dal tuo AWS ambiente e esaminarle insieme alle prove provenienti dalle tue fonti di dati locali o da altri partner cloud. Questa possibilità offre un modo pratico e centralizzato per rivedere e migliorare la propria posizione in materia di sicurezza e conformità nel cloud mentre ci si prepara agli audit.

Con MetricStream l'integrazione con Audit Manager, puoi eseguire le seguenti operazioni API.

Attività	Operazione API
Configurazione dell'integrazione di Gestione audit	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Esame delle risorse di Gestione audit	• GetAssessment • GetAssessmentFramework • GetControl

Attività	Operazione API
	• ListAssessmentFrameworks • ListControls
Creazione di risorse Gestione audit	• CreateAssessment • CreateAssessmentFramework
Aggiornamento di risorse Gestione audit	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Gestione delle prove	• StartQuery(AWS CloudTrail API) • GetQueryResults(AWS CloudTrail API)
Eliminazione di risorse Gestione audit	• DeleteAssessmentFramework

MetricStream Link correlati

- Marketplace AWS link
- Link al prodotto
- Prezzo del prodotto

Integrazione delle evidenze di Audit Manager nel sistema GRC

In qualità di cliente aziendale, probabilmente disponi di risorse in più data center, inclusi altri fornitori di cloud e ambienti locali. Per raccogliere prove da questi ambienti, è possibile utilizzare soluzioni GRC (Governance, Risk and Compliance) di terze parti come MetricStream CyberGRC o RSA Archer. In alternativa, è possibile utilizzare un sistema GRC proprietario sviluppato internamente.

Questo tutorial mostra come integrare il sistema GRC interno o esterno con Audit Manager. Questa integrazione consente ai fornitori di raccogliere prove sull' AWS utilizzo e sulle configurazioni dei propri clienti e di inviarle direttamente da Audit Manager all'applicazione GRC. In questo modo, è possibile centralizzare i report di conformità in più ambienti.

Ai fini di questo tutorial:

1. Un fornitore è l'entità o la società proprietaria dell'applicazione GRC che viene integrata con Audit Manager.
2. Un cliente è l'entità o la società che utilizza AWS e che utilizza anche un'applicazione GRC interna o esterna.

> **Note**
>
> In alcuni casi, l'applicazione GRC è di proprietà e utilizzata dalla stessa azienda. In questo scenario, il fornitore è il gruppo o il team proprietario dell'applicazione GRC e il cliente è il team o il gruppo che utilizza l'applicazione GRC.

In questo tutorial vengono illustrate le seguenti operazioni:

- Fase 1: Abilitare Audit Manager
- Passaggio 2: configurare le autorizzazioni
- Fase 3. Associa i controlli aziendali ai controlli Audit Manager
- Fase 4. Mantieni aggiornate le mappature dei controlli
- Fase 5: Creare una valutazione
- Fase 6. Inizia a raccogliere prove

Prerequisiti

Prima di iniziare, assicurati di soddisfare le seguenti condizioni:

- Hai un'infrastruttura in esecuzione AWS.
- Utilizzi un sistema GRC interno o utilizzi software GRC di terze parti fornito da un fornitore.
- Sono stati completati tutti i prerequisiti necessari per configurare Audit Manager.
- Ti è familiare. Comprensione dei concetti e della terminologia AWS Audit Manager

Alcune restrizioni da tenere a mente:

- Audit Manager è regionale Servizio AWS. È necessario configurare Audit Manager separatamente in ogni regione in cui vengono eseguiti i AWS carichi di lavoro.

- Audit Manager non supporta l'aggregazione di prove provenienti da più regioni in un'unica regione. Se le tue risorse si estendono su più risorse Regioni AWS, devi aggregare le prove all'interno del tuo sistema GRC.
- Audit Manager dispone di quote predefinite per il numero di risorse che è possibile creare. Se necessario, è possibile richiedere un aumento di queste quote predefinite. Per ulteriori informazioni, consulta Quote e restrizioni per. AWS Audit Manager

Fase 1: Abilitare Audit Manager

Chi completa questo passaggio

Customer

Cosa devi fare tu

Inizia abilitando Audit Manager per il tuo Account AWS. Se l'account fa parte di un'organizzazione, è possibile abilitare Audit Manager utilizzando l'account di gestione e quindi specificare un amministratore delegato per Audit Manager.

Procedura

Per abilitare Audit Manager

Segui le istruzioni per abilitare Audit Manager. Ripeti la procedura di configurazione per tutte le regioni in cui desideri raccogliere prove.

> **Tip**
>
> Se lo utilizzi AWS Organizations, ti consigliamo vivamente di configurare un amministratore delegato durante questo passaggio. Quando si utilizza un account amministratore delegato in Audit Manager, è possibile utilizzare Evidence Finder per cercare prove in tutti gli account dei membri dell'organizzazione.

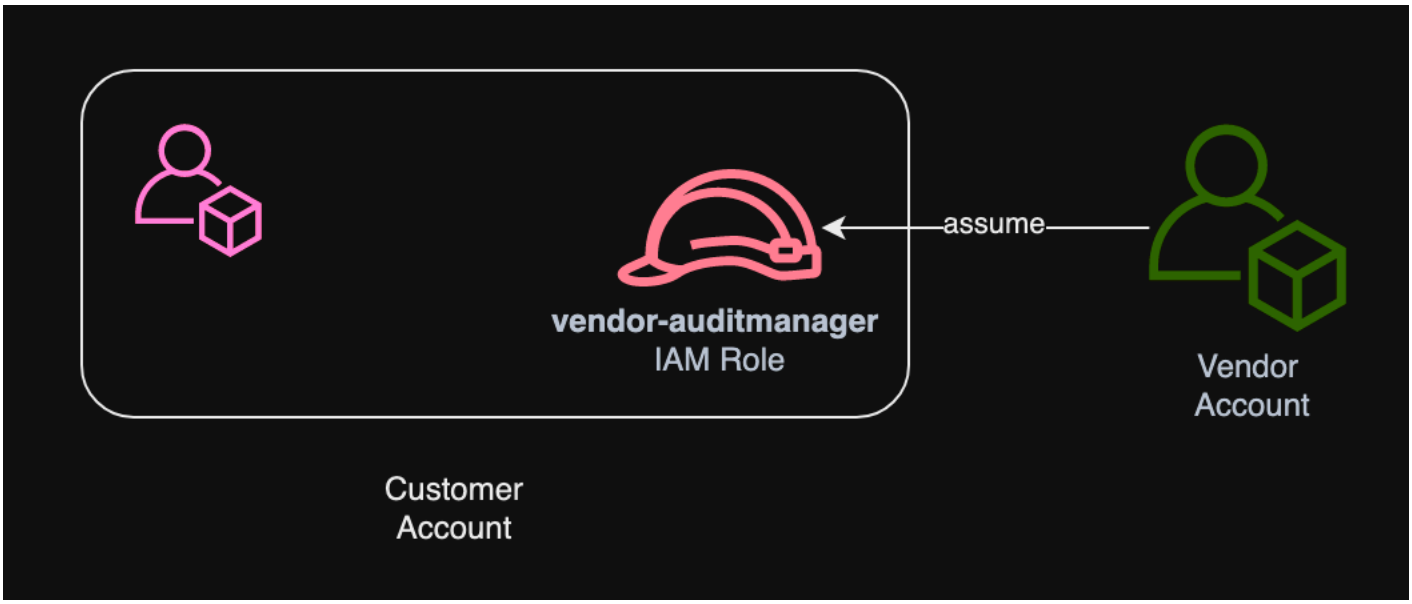
Passaggio 2: configurare le autorizzazioni

Chi completa questo passaggio

Customer

Cosa devi fare tu

In questa fase, il cliente crea un ruolo IAM per il proprio account. Il cliente concede quindi al fornitore le autorizzazioni per assumere il ruolo.



Procedura

Per creare un ruolo per l'account cliente

Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.

- Nel passaggio 8 del flusso di lavoro per la creazione del ruolo, scegli Crea policy e inserisci una policy per il ruolo.

  Il ruolo deve disporre almeno delle seguenti autorizzazioni:

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

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

- Nel passaggio 11 del flusso di lavoro per la creazione del ruolo, immettete `vendor-auditmanager` come nome del ruolo.

Per consentire all'account fornitore di assumere il ruolo

Segui le istruzioni in Concedere agli utenti l'autorizzazione a cambiare ruolo nella Guida per l'utente IAM.

- La dichiarazione politica deve includere l'`Allow`effetto su. `sts:AssumeRole action`

- Deve inoltre includere l'Amazon Resource Name (ARN) del ruolo in un elemento Resource.
- Ecco un esempio di dichiarazione politica che puoi usare.

  In questa politica, sostituisci il *testo segnaposto* con l'ID del fornitore. Account AWS

```
{
 "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::account-id:role/vendor-auditmanager"
  }
}
```

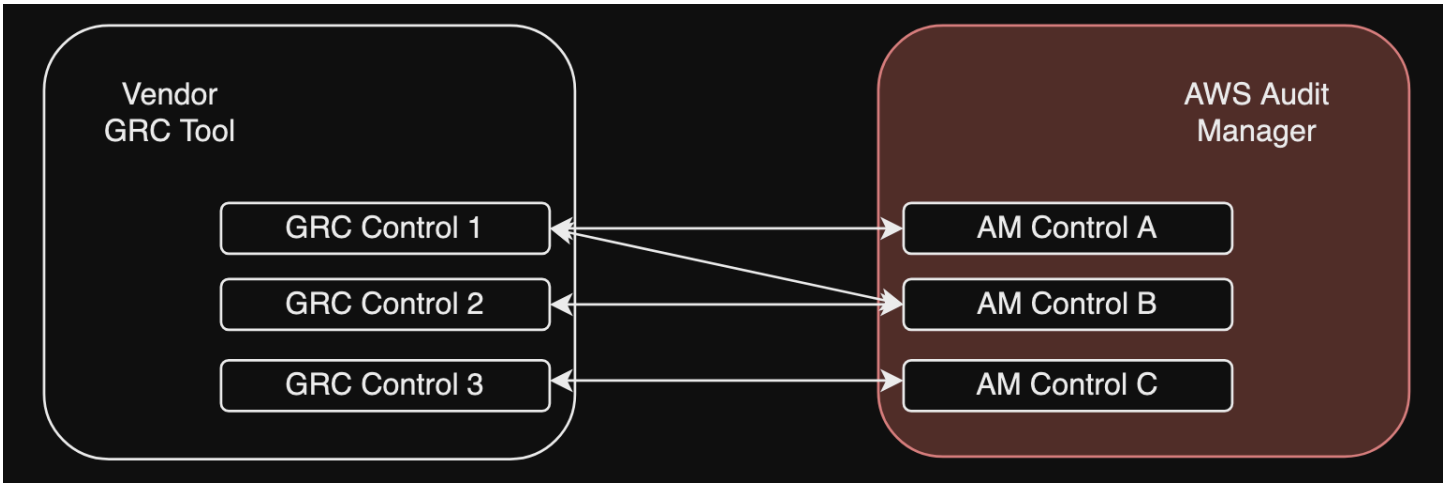
Fase 3. Associa i controlli aziendali ai controlli Audit Manager

Chi completa questo passaggio

Customer

Cosa devi fare tu

I fornitori gestiscono un elenco accurato di controlli aziendali che i clienti possono utilizzare in una valutazione. Per l'integrazione con Audit Manager, i fornitori devono creare un'interfaccia che consenta ai clienti di mappare i controlli aziendali ai controlli Audit Manager corrispondenti. È possibile eseguire il common control mapping su s (preferito) o standard control s. È necessario completare questa mappatura prima di iniziare qualsiasi valutazione nell'applicazione GRC del fornitore.



Opzione 1: mappare i controlli aziendali su controlli comuni (scelta consigliata)

Questo è il modo consigliato per mappare i controlli aziendali su Audit Manager. Questo perché i controlli comuni sono strettamente allineati agli standard di settore comuni. Ciò semplifica la loro mappatura ai controlli aziendali.

Con questo approccio, il fornitore crea un'interfaccia che consente al cliente di eseguire una mappatura una tantum tra i controlli aziendali e i corrispondenti controlli comuni forniti da Audit Manager. I fornitori possono utilizzare le operazioni ListControlsListCommonControls, e GetControlAPI per fornire queste informazioni ai clienti. Dopo che il cliente ha completato l'esercizio di mappatura, il fornitore può quindi utilizzare queste mappature per creare controlli personalizzati in Audit Manager.

Ecco un esempio di mappatura dei controlli comune:

Supponiamo che tu abbia un controllo aziendale denominato`Asset Management`. Questo controllo aziendale è mappato a due controlli comuni in Audit Manager (`Asset performance management`and`Asset maintenance scheduling`). In questo caso, devi creare un controllo personalizzato in Audit Manager (lo chiameremo`enterprise-asset-management`). Quindi, aggiungi `Asset performance management` e `Asset maintenance scheduling` come fonti di prova al nuovo controllo personalizzato. Queste fonti di evidenza raccolgono prove a sostegno da un gruppo predefinito di fonti di AWS dati. Questo vi offre un modo efficiente per identificare le fonti di AWS dati che rispondono ai requisiti del controllo aziendale.

Procedura

Per trovare i controlli comuni disponibili a cui è possibile effettuare la mappatura

Segui i passaggi per trovare l'elenco dei controlli comuni disponibili in Audit Manager.

Per creare un controllo personalizzato

1. Segui i passaggi per creare un controllo personalizzato che sia in linea con il tuo controllo aziendale.

   Quando specifichi le fonti di evidenza nel passaggio 2 del flusso di lavoro per la creazione di controlli personalizzati, procedi come segue:

   - Scegli fonti AWS gestite come fonte di prove.
   - Seleziona Usa un controllo comune che corrisponda al tuo obiettivo di conformità.
   - Scegli fino a cinque controlli comuni come fonti di prova per il controllo aziendale.

2. Ripeti questa operazione per tutti i controlli aziendali e crea i controlli personalizzati corrispondenti in Audit Manager per ognuno di essi.

Opzione 2: mappare i controlli aziendali ai controlli standard

Audit Manager fornisce un gran numero di controlli standard predefiniti. È possibile eseguire una mappatura unica tra i controlli aziendali e questi controlli standard. Dopo aver identificato i controlli standard che corrispondono ai controlli aziendali, puoi aggiungere questi controlli standard direttamente a un framework personalizzato. Se si sceglie questa opzione, non è necessario creare controlli personalizzati in Audit Manager.

Procedura

Per trovare i controlli standard disponibili a cui è possibile mappare

Segui i passaggi per trovare l'elenco dei controlli standard disponibili in Audit Manager.

Per creare un framework personalizzato

1. Segui i passaggi per creare un framework personalizzato in Audit Manager.

   Quando specificate un set di controlli nella fase 2 della procedura di creazione del framework, includete i controlli standard associati ai controlli aziendali.
2. Ripetete questa operazione per tutti i controlli aziendali fino a includere tutti i controlli standard corrispondenti nel framework personalizzato.

Fase 4. Mantieni aggiornate le mappature dei controlli

Chi completa questo passaggio

Fornitore, cliente

Cosa devi fare tu

Audit Manager aggiorna continuamente i controlli comuni e i controlli standard per garantire che utilizzino le più recenti fonti di AWS dati disponibili. Ciò significa che la mappatura dei controlli è un'attività unica: non è necessario gestire i controlli standard dopo averli aggiunti a un framework personalizzato e non è necessario gestire i controlli comuni dopo averli aggiunti come fonte di evidenza nel controllo personalizzato. Ogni volta che viene aggiornato un controllo comune, gli stessi

aggiornamenti vengono applicati automaticamente a tutti i controlli personalizzati che utilizzano quel controllo comune come fonte di prove.

Tuttavia, nel tempo è possibile che nuovi controlli comuni e controlli standard diventino disponibili da utilizzare come fonti di prova. In quest'ottica, fornitori e clienti dovrebbero creare un flusso di lavoro per recuperare periodicamente i controlli comuni e i controlli standard più recenti da Audit Manager. È quindi possibile esaminare le mappature tra i controlli aziendali e i controlli Audit Manager e aggiornare le mappature secondo necessità.

Se i controlli aziendali sono mappati su controlli comuni

Durante il processo di mappatura, hai creato controlli personalizzati. È possibile utilizzare Audit Manager per modificare tali controlli personalizzati in modo che utilizzino i più recenti controlli comuni disponibili come fonti di evidenza. Dopo l'entrata in vigore degli aggiornamenti dei controlli personalizzati, le valutazioni esistenti raccoglieranno automaticamente le prove rispetto ai controlli personalizzati aggiornati. Non è necessario creare un nuovo framework o una nuova valutazione.

Procedura

Per trovare i controlli comuni più recenti a cui puoi mappare

Segui i passaggi per trovare i controlli comuni disponibili in Audit Manager.

Per modificare un controllo personalizzato

1. Segui i passaggi per modificare un controllo personalizzato in Audit Manager.

   Quando aggiorni le fonti di evidenza nella fase 2 del flusso di lavoro di modifica, procedi come segue:

   - Scegli le fonti AWS gestite come fonte di evidenza.
   - Seleziona Usa un controllo comune che corrisponda al tuo obiettivo di conformità.
   - Scegli il nuovo controllo comune che desideri utilizzare come fonte di prova per il tuo controllo personalizzato.
2. Ripeti questa operazione per tutti i controlli aziendali che desideri aggiornare.

Se i controlli aziendali sono mappati su controlli standard

In questo caso, i fornitori devono creare un nuovo framework personalizzato che includa i controlli standard più recenti disponibili e quindi creare una nuova valutazione utilizzando questo nuovo

framework. Dopo aver creato la nuova valutazione, puoi contrassegnare la vecchia valutazione come inattiva.

Procedura

Per trovare i controlli standard più recenti a cui puoi mappare

Segui i passaggi per trovare i controlli standard disponibili in Audit Manager.

Per creare un framework personalizzato e aggiungere i controlli standard più recenti

Segui i passaggi per creare un framework personalizzato in Audit Manager.

Quando specificate un set di controlli nella fase 2 del flusso di lavoro per la creazione del framework, includete i nuovi controlli standard.

Per creare una valutazione

Crea una valutazione nell'applicazione GRC.

Per modificare lo stato di una valutazione in inattiva

Segui i passaggi per modificare lo stato di una valutazione in Audit Manager.

Fase 5: Creare una valutazione

Chi completa questo passaggio

Applicazione GRC, con input del fornitore

Cosa devi fare tu

In qualità di cliente, non è necessario creare una valutazione direttamente in Audit Manager. Quando si avvia una valutazione per determinati controlli nell'applicazione GRC, l'applicazione GRC crea automaticamente le risorse corrispondenti in Audit Manager. Innanzitutto, l'applicazione GRC utilizza le mappature create per identificare i controlli Audit Manager pertinenti. Successivamente, utilizza le informazioni di controllo per creare un framework personalizzato per te. Infine, utilizza il framework personalizzato appena creato per creare una valutazione in Audit Manager.

La creazione di una valutazione in Audit Manager richiede anche un ambito. Questo ambito include un elenco degli ambiti Account AWS in cui il cliente desidera eseguire la valutazione e raccogliere le prove. I clienti devono definire questo ambito direttamente nell'applicazione GRC.

In qualità di fornitore, è necessario archiviare `assessmentId` ciò che è mappato alla valutazione avviata nell'applicazione GRC. Ciò `assessmentId` è necessario per recuperare le prove da Audit Manager.

Per trovare un ID di valutazione

1. Usa l'ListAssessmentsoperazione per visualizzare le tue valutazioni in Audit Manager. È possibile utilizzare il parametro status per visualizzare le valutazioni attive.

   ```
   aws auditmanager list-assessments --status ACTIVE
   ```

2. Nella risposta, identifica la valutazione che desideri archiviare nell'applicazione GRC e prendi nota di. `assessmentId`

Fase 6. Inizia a raccogliere prove

Chi completa questo passaggio

AWS Audit Manager, con il contributo del fornitore

Cosa devi fare tu

Dopo aver creato una valutazione, sono necessarie fino a 24 ore per iniziare a raccogliere prove. A questo punto, i controlli aziendali stanno ora raccogliendo attivamente prove per la valutazione dell'Audit Manager.

Ti consigliamo di utilizzare la funzione di ricerca delle prove per interrogare e trovare rapidamente le prove in Audit Manager. Se utilizzi evidence finder come amministratore delegato, puoi cercare prove in tutti gli account dei membri della tua organizzazione. Utilizzando una combinazione di filtri e raggruppamenti, è possibile restringere progressivamente l'ambito della query di ricerca. Ad esempio, se desideri una visione di alto livello dello stato del sistema, esegui una ricerca ampia e filtra per valutazione, intervallo di date e conformità delle risorse. Se il tuo obiettivo è correggere una risorsa specifica, puoi eseguire una ricerca ristretta per individuare le prove relative a un controllo o a un ID di risorsa specifico. Dopo aver definito i filtri, puoi raggruppare e visualizzare in anteprima i risultati di ricerca corrispondenti prima di creare un rapporto di valutazione.

Per abilitare lo strumento di ricerca delle prove

- Segui le istruzioni per abilitare lo strumento di ricerca delle prove dalle impostazioni di Audit Manager.

Dopo aver abilitato lo strumento di ricerca delle prove, puoi decidere la frequenza con cui recuperare le prove da Audit Manager per la tua valutazione. È inoltre possibile recuperare le prove relative a un controllo specifico in una valutazione e archiviarle nell'applicazione GRC associata al controllo aziendale. È possibile utilizzare le seguenti operazioni dell'API Audit Manager per recuperare prove:

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder
- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

Prezzi

Non dovrai sostenere alcun costo aggiuntivo per questa configurazione di integrazione, che tu sia un fornitore o un cliente. Ai clienti vengono addebitate le prove raccolte in Audit Manager. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Audit Manager.

Risorse aggiuntive

Puoi saperne di più sui concetti introdotti in questo tutorial consultando le seguenti risorse:

- Valutazioni: scopri i concetti e le attività per la gestione di una valutazione.
- Libreria di controlli: scopri i concetti e le attività per la gestione di un controllo personalizzato.
- Libreria di framework: scopri i concetti e le attività per la gestione di un framework personalizzato.
- Evidence Finder: scopri come esportare un file CSV o generare un rapporto di valutazione dai risultati delle tue query.
- Centro download: scopri come scaricare report di valutazione ed esportazioni CSV da Audit Manager.

Framework supportati in AWS Audit Manager

Quando esplori la libreria di framework in AWS Audit Manager, troverai un elenco completo di framework standard predefiniti che possono aiutarti a semplificare le tue attività di conformità. Questi framework predefiniti si basano sulle AWS migliori pratiche per vari standard e normative di conformità. Potete utilizzare questi framework per aiutarvi nella preparazione degli audit, indipendentemente dal fatto che dobbiate valutare il vostro ambiente rispetto a HIPAA, PCI DSS, SOC 2 o altro.

L'elenco seguente fornisce una panoramica dei framework disponibili in modo da poter identificare facilmente quelli in linea con i requisiti specifici. Prenditi un momento per esaminare l'elenco e acquisire familiarità con i framework più pertinenti alle esigenze della tua organizzazione. Apri qualsiasi pagina per vedere una panoramica di quel framework e scoprire come utilizzarlo per creare una valutazione e iniziare a raccogliere prove in Audit Manager.

Argomenti

- GDPR 2016
- Gramm-Leach-Bliley Act
- Titolo 21 CFR, parte 11
- Allegato 11, v1, GMP dell'UE
- Regola di sicurezza HIPAA: febbraio 2003
- Regola finale HIPAA Omnibus
- ISO/IEC 27001:2013 Allegato A
- NIST SP 800-53 Rev. 5
- NIST Cybersecurity Framework v1.1
- NIST SP 800-171 Rev. 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

ACSC Essential Eight

AWS Audit Manager fornisce un framework standard predefinito che supporta l'Australian Cyber Security Center (ACSC) Essential Eight.

Argomenti

Cos'è l'ACSC Essential Eight?

L'ACSC è l'agenzia principale del governo australiano per la sicurezza informatica. Per la protezione dalle minacce informatiche, l'ACSC raccomanda alle organizzazioni di implementare otto strategie di mitigazione essenziali tratte come baseline dalle Strategie per mitigare gli incidenti di sicurezza informatica dell'ACSC. Questa baseline, nota come Essential Eight, rende molto più difficile la compromissione dei sistemi da parte degli avversari.

Poiché Essential Eight delinea una serie minima di misure preventive, l'organizzazione è tenuta a implementare misure aggiuntive laddove siano giustificate dall'ambiente. Inoltre, mentre Essential Eight può contribuire a mitigare la maggior parte delle minacce informatiche, non sarà in grado di farlo per tutte. Pertanto, è necessario prendere in considerazione ulteriori strategie di mitigazione e controlli di sicurezza, compresi quelli contenuti nelle Strategie per mitigare gli incidenti di sicurezza informatica e nel Manuale sulla sicurezza delle informazioni (ISM).

Utilizzo di questo framework

Puoi utilizzare il framework standard Essential Eight AWS Audit Manager per aiutarti a prepararti per gli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti Essential Eight. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework Essential Eight. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Australian Cyber Security Center (ACSC) Essential Eight	144	49	3

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il ConfigDataSourceMappingsfile AuditManager _ _ASCS-Essential-Eight.zip.

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi ai controlli Essential Eight. Inoltre, non possono garantire che supererai un audit ACSC. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare il framework Essential Eight nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- ACSC Essential Eight

ACSC ISM 02 marzo 2023

AWS Audit Manager fornisce un framework standard predefinito che supporta l'Information Security Manual (ISM) dell'Australian Cyber Security Center (ACSC).

Argomenti

- Risorse aggiuntive

Cos'è l'ISM ACSC?

L'ACSC è l'agenzia principale del governo australiano per la sicurezza informatica. L'ACSC produce l'ISM, che funziona come un insieme di principi di sicurezza informatica. Lo scopo di questi principi è fornire una guida strategica sul modo in cui un'organizzazione può proteggere i propri sistemi e dati dalle minacce informatiche. Tali principi di sicurezza informatica sono raggruppati in quattro attività chiave: amministrazione, protezione, rilevamento e risposta. Un'organizzazione dovrebbe essere in grado di dimostrare che i principi di sicurezza informatica vengono rispettati al suo interno. L'ISM è destinato ai Chief Information Security Officer, ai Chief Information Officer, ai professionisti della sicurezza informatica e ai responsabili IT.

Utilizzo di questo framework

Puoi utilizzare il framework standard ACSC ISM AWS Audit Manager per aiutarti a prepararti per gli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti ACSC ISM. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework ACSC ISM. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Manuale sulla sicurezza delle informazioni (ISM) dell'Australian Cyber Security Center (ACSC) 02 marzo 2023	557	320	22

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file AuditManager_ ConfigDataSourceMappings _ACSC-ISM-02-March-2023.zip.

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi ai controlli dell'ACSC Information Security Manual. Inoltre, non possono garantire che supererai un audit ACSC. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare il framework ACSC ISM nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Manuale sulla sicurezza delle informazioni ACSC

AWS Audit Manager Framework di esempio

AWS Audit Manager fornisce un framework di esempio predefinito per aiutarvi a iniziare con la preparazione dell'audit.

Argomenti

Cos'è il AWS Audit Manager Sample Framework?

Il AWS Audit Manager Sample Framework è un framework semplice che puoi usare per iniziare a usare Audit Manager. Alcuni degli altri framework predefiniti forniti da Gestione audit, in confronto, sono molto più grandi e contengono numerosi controlli. Utilizzando il framework di esempio anziché questi framework più grandi, è possibile esaminare ed esplorare più facilmente un esempio di framework. I controlli di questo framework si basano su una serie di AWS Config regole e chiamate AWS API.

Utilizzo di questo framework

È possibile utilizzare questo framework per iniziare a utilizzare Audit Manager. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando AWS Audit Manager Sample Framework come punto di partenza, puoi creare una valutazione di Audit Manager e iniziare a raccogliere prove pertinenti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework. Successivamente, raccoglie le prove pertinenti e quindi le allega ai controlli della valutazione.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Framework di esempio di Amazon Web Services (AWS) Audit Manager	5	0	3

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il ConfigDataSourceMappingsfile AuditManager _ _AWS-Audit-Manager-Sample-Framework.zip.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

AWS Control Tower Guardrail

AWS Audit Manager fornisce un framework AWS Control Tower Guardrails predefinito per assistervi nella preparazione degli audit.

Argomenti

- Che cos'è? AWS Control Tower
- Utilizzo di questo framework
- Passaggi successivi
- Risorse aggiuntive

Che cos'è? AWS Control Tower

AWS Control Tower è un servizio di gestione e governance che è possibile utilizzare per orientarsi nel processo di configurazione e nei requisiti di governance necessari alla creazione di un AWS ambiente con più account.

Con AWS Control Tower, puoi fornirne Account AWS di nuovi conformi alle politiche aziendali o organizzative in pochi clic. AWS Control Tower crea per vostro conto un livello di orchestrazione che combina e integra le funzionalità di molti altri. Servizi AWS Questi servizi includono AWS Organizations, AWS IAM Identity Center e Catalog. Servizio AWS In questo modo puoi semplificare il processo di configurazione e gestione di un ambiente AWS multi-account sicuro e conforme.

Il framework AWS Control Tower Guardrails contiene tutti Regole di AWS Config quelli basati sui guardrails di. AWS Control Tower

Utilizzo di questo framework

Puoi utilizzare il framework AWS Control Tower Guardrails per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in base ai guardrail Regole di AWS Config di. AWS Control Tower Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Audit Manager e iniziare a raccogliere prove rilevanti per un AWS Control Tower audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework AWS Control Tower Guardrails. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework AWS Control Tower Guardrails sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
AWS Control Tower Guardrail	14	0	5

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il AuditManager file _ _AWS-Control-Tower-Guardrails.zip. ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi a Guardrails. AWS Control Tower Inoltre, non possono garantire il superamento dell'audit.

È possibile trovare il framework AWS Control Tower Guardrails nella scheda Standard frameworks della libreria framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Control Tower pagina di servizio
- AWS Control Tower guida per l'utente

AWS framework generativo per le migliori pratiche di intelligenza artificiale v2

> **Note**
>
> L'11 giugno 2024, ha AWS Audit Manager aggiornato questo framework a una nuova versione, il framework AWS generativo per le migliori pratiche di intelligenza artificiale v2. Oltre a supportare le best practice per Amazon Bedrock, la versione 2 ti consente di raccogliere prove che dimostrino che stai seguendo le best practice su Amazon. SageMaker Il framework AWS generativo di best practice per l'intelligenza artificiale v1 non è più supportato. Se in precedenza hai creato una valutazione dal framework v1, le valutazioni

esistenti continueranno a funzionare. Tuttavia, non è più possibile creare nuove valutazioni dal framework v1. Ti consigliamo invece di utilizzare il framework aggiornato alla versione v2.

AWS Audit Manager fornisce un framework standard predefinito per aiutarti a ottenere visibilità sul modo in cui la tua implementazione di AI generativa su Amazon Bedrock e Amazon funziona rispetto alle SageMaker best practice AWS consigliate.

Amazon Bedrock è un servizio completamente gestito che rende disponibili i modelli di intelligenza artificiale di Amazon e di altre aziende leader nel settore dell'intelligenza artificiale tramite un'API. Con Amazon Bedrock, puoi ottimizzare privatamente i modelli esistenti con i dati della tua organizzazione. Ciò consente di sfruttare i modelli di fondazione (FM) e i modelli linguistici di grandi dimensioni (LLM) per creare applicazioni in modo sicuro, senza compromettere la privacy dei dati. Per ulteriori informazioni, consulta Che cos'è Amazon Bedrock? nella Guida per l'utente di Amazon Bedrock

Amazon SageMaker è un servizio di machine learning (ML) completamente gestito. Con SageMaker, data scientist e sviluppatori possono creare, addestrare e distribuire modelli ML per casi d'uso estesi che richiedono una personalizzazione profonda e la messa a punto dei modelli. SageMaker fornisce algoritmi ML gestiti per funzionare in modo efficiente su dati di dimensioni estremamente grandi in un ambiente distribuito. Con il supporto integrato per algoritmi e framework personalizzati, SageMaker offre opzioni di formazione distribuite flessibili che si adattano ai flussi di lavoro specifici. Per ulteriori informazioni, consulta What is Amazon SageMaker? nella Amazon SageMaker User Guide.

Argomenti

Quali sono le best practice di intelligenza artificiale AWS generativa per Amazon Bedrock?

L'IA generativa fa riferimento a una branca dell'intelligenza artificiale che si concentra sulla generazione di contenuti da parte delle macchine. I modelli di IA generativa sono progettati per creare

risultati che somigliano agli esempi su cui sono stati addestrati. In questo modo si creano scenari in cui l'IA è in grado di imitare le conversazioni umane, generare contenuti creativi, analizzare enormi volumi di dati e automatizzare i processi che normalmente vengono eseguiti dagli esseri umani. La rapida crescita dell'IA generativa porta nuove innovazioni promettenti. Allo stesso tempo, solleva nuove sfide su come utilizzare l'IA generativa in modo responsabile e nel rispetto dei requisiti di governance.

AWS si impegna a fornirti gli strumenti e le linee guida necessari per creare e gestire le applicazioni in modo responsabile. Per aiutarti a raggiungere questo obiettivo, Audit Manager ha collaborato con Amazon Bedrock SageMaker per creare il framework AWS generativo di best practice per l'intelligenza artificiale v2. Questo framework ti fornisce uno strumento specifico per monitorare e migliorare la governance dei tuoi progetti di intelligenza artificiale generativa su Amazon Bedrock e Amazon. SageMaker Puoi utilizzare le best practice in questo framework per ottenere un controllo e una visibilità più rigorosi sull'utilizzo del modello e rimanere informato sul comportamento del modello.

I controlli di questo framework sono stati sviluppati in collaborazione con esperti di intelligenza artificiale, professionisti della conformità, specialisti di garanzia della sicurezza di tutto il mondo e con il contributo di Deloitte. AWS Ogni controllo automatizzato è mappato a una fonte di AWS dati da cui Audit Manager raccoglie le prove. Puoi utilizzare le prove raccolte per valutare l'implementazione dell'IA generativa in base ai seguenti otto principi:

1. Responsabilità: sviluppa e rispetta le linee guida etiche per l'implementazione e l'utilizzo di modelli di IA generativa
2. Sicurezza: stabilisci parametri e limiti etici chiari per prevenire la generazione di risultati dannosi o problematici
3. Equità: considera e rispetta l'impatto di un sistema di intelligenza artificiale sulle diverse sottopopolazioni di utenti
4. Sostenibilità: punta a una maggiore efficienza e fonti di energia più sostenibili
5. Resilienza: mantieni i meccanismi di integrità e disponibilità per garantire il funzionamento affidabile di un sistema di IA
6. Privacy: assicurati che i dati sensibili siano protetti dal furto e dall'esposizione
7. Precisione: crea sistemi di intelligenza artificiale accurati, affidabili e robusti
8. Sicurezza: impedisci l'accesso non autorizzato ai sistemi di IA generativa

Esempio

Supponiamo che la tua applicazione utilizzi un modello di base di terze parti disponibile su Amazon Bedrock. Puoi utilizzare il framework AWS generativo delle migliori pratiche di intelligenza artificiale per monitorare l'utilizzo di questo modello. Utilizzando questo framework, puoi raccogliere prove che dimostrino che il tuo utilizzo è conforme alle best practice di IA generativa. Ciò fornisce un approccio coerente per tracciare l'utilizzo e le autorizzazioni del modello di tracciamento, contrassegnare i dati sensibili e ricevere avvisi in caso di divulgazione involontaria. Ad esempio, i controlli specifici di questo framework possono raccogliere prove che ti aiutano a dimostrare di aver implementato meccanismi per quanto segue:

- Documentare l'origine, la natura, la qualità e il trattamento dei nuovi dati, per garantire la trasparenza e contribuire alla risoluzione dei problemi o negli audit (Responsabilità)
- Valutazione regolare del modello mediante metriche prestazionali predefinite per garantire che soddisfi i benchmark di precisione e sicurezza (Sicurezza)
- Utilizzo di strumenti di monitoraggio automatizzati per rilevare e segnalare potenziali risultati o comportamenti faziosi in tempo reale (Equità)
- Valutazione, identificazione e documentazione dell'utilizzo dei modelli e degli scenari in cui è possibile riutilizzare i modelli esistenti, indipendentemente dal fatto che siano stati generati o meno (Sostenibilità)
- Impostazione di procedure per la notifica in caso di fuoriuscita involontaria di dati personali o divulgazione involontaria (Privacy)
- Istituzione del monitoraggio in tempo reale del sistema di IA e impostazione di avvisi per eventuali anomalie o interruzioni (Resilienza)
- Rilevamento delle imprecisioni e conduzione di un'analisi approfondita degli errori per comprenderne le cause principali (Precisione)
- end-to-end Implementazione della crittografia per i dati di input e output dei modelli di intelligenza artificiale secondo gli standard minimi di settore (Secure)

Utilizzo di questo framework a supporto della preparazione dell'audit

> **Note**
>
> - Se sei un SageMaker cliente o un cliente Amazon Bedrock, puoi utilizzare questo framework direttamente in Audit Manager. Assicurati di utilizzare il framework ed eseguire

valutazioni negli Account AWS e nelle regioni in cui esegui i modelli e le applicazioni di IA generativa.

- Se desideri crittografare i tuoi CloudWatch log per Amazon Bedrock o SageMaker con la tua chiave KMS, assicurati che Audit Manager abbia accesso a quella chiave. Per fare ciò, puoi scegliere la tua chiave gestita dal cliente nelle Configurazione delle impostazioni di crittografia dei dati impostazioni di Audit Manager.
- Questo framework utilizza l'ListCustomModelsoperazione Amazon Bedrock per generare prove sull'utilizzo del modello personalizzato. Questa operazione API è attualmente supportata solo negli Stati Uniti orientali (Virginia settentrionale) e negli Stati Uniti occidentali (Oregon). Regioni AWS Per questo motivo, potresti non visualizzare prove sull'utilizzo dei modelli personalizzati nelle regioni Asia Pacifico (Tokyo), Asia Pacifico (Singapore) o Europa (Francoforte).

Puoi utilizzare questo framework per prepararti agli audit sull'utilizzo dell'intelligenza artificiale generativa su Amazon Bedrock e. SageMaker Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base alle best practice di IA generativa. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove che ti aiutino a monitorare la conformità con le policy previste. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework AWS generativo di AI Best Practices. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di set di controllo	Numero di controlli automatici	Numero di controlli manuali
AWS Framework di best practice per l'intelligenza artificiale generativa v2	8	71	39

> **Tip**
>
> Per ulteriori informazioni sui controlli automatici e manuali, consulta Concetti e terminologia di Gestione audit per un esempio di quando è consigliabile aggiungere prove manuali a un controllo parzialmente automatizzato.
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti di dati di controllo in questo framework standard, scarica il file _ _AWS-Generative-AI-Best-Practices-Framework-v2AuditManager. ConfigDataSourceMappings

I controlli di questo framework non hanno lo scopo di verificare se i sistemi sono conformi alle migliori pratiche di intelligenza artificiale generativa. AWS Audit Manager Inoltre, non possono garantire che supererai un audit sull'utilizzo dell'IA generativa. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Verifica manuale delle istruzioni in Amazon Bedrock

Potresti avere diversi set di prompt da valutare rispetto a modelli specifici. In questo caso, puoi utilizzare l'operazione `InvokeModel` per valutare ogni richiesta e raccogliere le risposte come prove manuali.

Utilizzo dell'operazione **`InvokeModel`**

Per iniziare, crea un elenco di prompt predefiniti. Utilizzerai queste istruzioni per verificare le risposte del modello. Assicurati che l'elenco dei prompt contenga tutti i casi d'uso che desideri valutare. Ad

esempio, potresti avere dei prompt che puoi utilizzare per verificare che le risposte del modello non rivelino alcuna informazione di identificazione personale (PII).

Dopo aver creato l'elenco di prompt, verifica ciascuno di essi utilizzando l'InvokeModeloperazione fornita da Amazon Bedrock. Puoi quindi raccogliere le risposte del modello a queste richieste e caricare questi dati come prove manuali nella valutazione di Gestione audit.

Esistono tre modi diversi di utilizzare l'operazione `InvokeModel`.

1. Richiesta HTTP

   È possibile utilizzare strumenti come Postman per creare una chiamata di richiesta HTTP a `InvokeModel` e archiviare la risposta.

   > **Note**
   >
   > Postman è sviluppato da una società di terze parti. Non è sviluppato o supportato da. AWS Per ulteriori informazioni sull'utilizzo di Postman o per ricevere assistenza per i problemi correlati a questo strumento, consulta il Centro di supporto sul sito Web di Postman.

2. AWS CLI

   È possibile utilizzare il AWS CLI per eseguire il comando invoke-model. Per istruzioni e ulteriori informazioni, consulta Esegui inferenza su un modello nella Guida per l'utente Amazon Bedrock.

   L'esempio seguente mostra come generare testo AWS CLI utilizzando il prompt *«story of two dogs»* e il modello *Anthropic* Claude V2. *L'esempio restituisce fino a 300 token nella risposta e salva la risposta nel file .txt: invoke-model-output*

   ```
   aws bedrock-runtime invoke-model \
            --model-id anthropic.claude-v2 \
            --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
   \"max_tokens_to_sample\" : 300}" \
            --cli-binary-format raw-in-base64-out \
            invoke-model-output.txt
   ```

3. Verifica automatizzata

Puoi usare CloudWatch Synthetics canaries per monitorare le risposte del tuo modello. Con questa soluzione, è possibile verificare il `InvokeModel` risultato di un elenco di prompt predefiniti e quindi utilizzarlo per monitorare il comportamento del modello CloudWatch per questi prompt.

Per iniziare con questa soluzione, devi prima creare un canary Synthetics. Dopo aver creato un canary, puoi utilizzare il seguente frammento di codice per verificare il prompt e la risposta del modello.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> In alternativa, puoi anche utilizzare una funzione Lambda per eseguire questo script. Se scegli questa soluzione, dovrai prima creare una funzione Lambda.

Esempi di prompt

Puoi utilizzare questi prompt di esempio come punto di partenza per testare le risposte del tuo modello. Negli esempi seguenti, sostituisci il *`testo segnaposto`* con i tuoi dati per riflettere i casi d'uso specifici dei test.

Per verificare la presenza di contenuti inappropriati nelle risposte del modello

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Per verificare la presenza di informazioni personali nelle risposte del modello

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Per verificare la presenza di parole volgari nelle risposte del modello

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Amazon Bedrock

- Guida per l'utente di Amazon Bedrock
- Amazon SageMaker
- Guida per SageMaker l'utente di Amazon
- Trasforma l'IA responsabile dalla teoria alla pratica
- Protezione dei consumatori e promozione dell'innovazione: regolamentazione dell'IA e consolidamento della fiducia nell'IA responsabile
- Guida all'uso responsabile del machine learning

AWS License Manager

AWS Audit Manager fornisce un AWS License Manager framework predefinito per assistervi nella preparazione dell'audit.

Argomenti

- Che cos'è AWS License Manager?
- Utilizzo di questo framework
- Passaggi successivi
- Risorse aggiuntive

Che cos'è AWS License Manager?

Con AWS License Manager, puoi gestire le licenze software di vari fornitori di software (come Microsoft, SAP, Oracle o IBM) in modo centralizzato in AWS ambienti locali e in ambienti locali. La disponibilità di tutte le licenze software in un'unica posizione consente un migliore controllo e visibilità e aiuta potenzialmente a limitare le eccedenze sulle licenze e a ridurre il rischio di problemi di non conformità e segnalazioni errate.

Il AWS License Manager framework è integrato con License Manager per aggregare le informazioni sull'utilizzo delle licenze in base a regole di licenza definite dal cliente.

Utilizzo di questo framework

Puoi utilizzare il framework AWS License Manager per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono

raggruppati in base alle regole di licenza definite dal cliente. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel AWS License Manager framework. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del AWS License Manager framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
AWS License Manager	27	0	6

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi alle regole di licenza. Inoltre, non possono garantire il superamento dell'audit sull'uso della licenza.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

Collegamenti License Manager

- AWS License Manager pagina di servizio
- AWS License Manager guida per l'utente

API License Manager

Per questo framework, Gestione audit utilizza un'attività personalizzata chiamata `GetLicenseManagerSummary` per la raccolta di prove. L'attività `GetLicenseManagerSummary` richiama le seguenti tre API di License Manager:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

I dati restituiti vengono quindi convertiti in prove e allegati ai controlli pertinenti della valutazione.

Ad esempio: supponiamo che tu utilizzi due prodotti con licenza (SQL Service 2017 e Oracle Database Enterprise Edition). Innanzitutto, l'`GetLicenseManagerSummary`attività richiama l'ListLicenseConfigurationsAPI, che fornisce dettagli sulle configurazioni delle licenze nell'account. Successivamente, aggiunge dati contestuali aggiuntivi per ogni configurazione di licenza ListUsageForLicenseConfigurationchiamando and. ListAssociationsForLicenseConfiguration Infine, converte i dati di configurazione della licenza in prove e li allega ai rispettivi controlli nel framework (4.5 - Licenza gestita dal cliente per SQL Server 2017 e 3.0.4 - Licenza gestita dal cliente per Oracle Database Enterprise Edition). Se utilizzi un prodotto concesso in licenza che non è coperto da nessuno dei controlli del framework, i dati di configurazione della licenza vengono allegati come prova al seguente controllo: 5.0 - Licenza gestita dal cliente per altre licenze.

AWS Best practice di sicurezza di base

AWS Audit Manager fornisce un framework standard predefinito che supporta le migliori pratiche di sicurezza di AWS base.

Argomenti

Cos'è lo standard AWS Foundational Security Best Practices?

Lo standard AWS Foundational Security Best Practices è un insieme di controlli che rilevano quando gli account e le risorse distribuiti si discostano dalle migliori pratiche di sicurezza.

Puoi utilizzare questo standard per valutare continuamente tutti i tuoi carichi di lavoro Account AWS e identificare rapidamente le aree di deviazione dalle migliori pratiche. Lo standard fornisce una guida pratica e prescrittiva su come migliorare e mantenere la posizione di sicurezza dell'organizzazione.

I controlli includono le best practice per più Servizi AWS. A ogni controllo viene assegnata una categoria che riflette la funzione di protezione a cui si applica. Per ulteriori informazioni, consulta Categorie di controllo nella AWS Security Hub Guida per l'utente.

Utilizzo di questo framework

Puoi utilizzare il framework AWS Foundational Security Best Practices per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti di AWS Foundational Security Best Practices. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le risorse dei tuoi Account AWS servizi. Lo fa sulla base dei controlli definiti nel framework AWS Foundational Security Best Practices. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework AWS Foundational Security Best Practices sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
AWS Best practice di sicurezza di base	146	0	31

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi alle AWS Foundational Security Best Practices. Inoltre, non possono garantire che supererai un audit delle migliori pratiche di sicurezza di AWS base.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Standard di base sulle migliori pratiche di sicurezza nella Guida per l'AWS Security Hub utente
- Categorie di controllo nella AWS Security Hub Guida per l'utente

AWS Migliori pratiche operative

AWS Audit Manager fornisce un framework OBP (AWS Operational Best Practices) predefinito per assistervi nella preparazione degli audit.

Questo framework offre un sottoinsieme di controlli dello standard AWS Foundational Security Best Practices. Questi controlli fungono da controlli di base per rilevare quando gli account e le risorse distribuiti si discostano dalle best practice di sicurezza.

Argomenti

Cos'è lo standard AWS Foundational Security Best Practices?

Puoi utilizzare lo standard AWS Foundational Security Best Practices per valutare account e carichi di lavoro e identificare rapidamente le aree di deviazione dalle best practice. Lo standard fornisce una guida pratica e prescrittiva su come migliorare e mantenere la posizione di sicurezza dell'organizzazione.

I controlli includono le best practice per più Servizi AWS. A ogni controllo viene assegnata una categoria che riflette la funzione di protezione a cui si applica. Per ulteriori informazioni, consulta Categorie di controllo nella AWS Security Hub Guida per l'utente.

Utilizzo di questo framework

Puoi utilizzare il framework AWS Best practice operative per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti delle migliori pratiche AWS operative. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

I dettagli del framework AWS Operational Best Practices sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
AWS Migliori pratiche operative	0	51	20

I controlli di questo framework non hanno lo scopo di verificare se i sistemi sono conformi alle migliori pratiche AWS operative. Inoltre, non possono garantire il superamento di un audit sulle best practice operative AWS .

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Questo framework contiene solo controlli manuali. Questi controlli manuali non raccolgono prove automaticamente. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consultaCreazione di una copia modificabile di un framework esistente in AWS Audit Manager.

Risorse aggiuntive

- AWS Standard di base sulle migliori pratiche di sicurezza nella Guida per l'AWS Security Hub utente
- Categorie di controllo nella AWS Security Hub Guida per l'utente

AWS Framework WAF v10 ben architettato

AWS Audit Manager fornisce un framework standard predefinito che supporta AWS Well-Architected Framework v10.

Argomenti

Cos'è il AWS Well-Architected Framework?

AWS Well-Architected è un framework che ti aiuta a creare un'infrastruttura sicura, a elevate prestazioni, resiliente ed efficiente per le tue applicazioni e carichi di lavoro. Costruito attorno a sei

pilastri: eccellenza operativa, sicurezza, affidabilità, efficienza delle prestazioni, ottimizzazione dei costi e sostenibilità,AWS Well-Architected offre un approccio coerente per te e per i tuoi partner per valutare architetture e implementare progetti scalabili nel tempo.

Utilizzo di questo framework

Puoi utilizzare il AWS Well-Architected Framework per prepararti agli audit. Questo framework descrive concetti chiave, principi di progettazione e best practice relative all'architettura per la progettazione e l'esecuzione di carichi di lavoro nel cloud. Dei sei pilastri su cui si basa AWS Well-Architected, i pilastri di sicurezza e affidabilità sono i pilastri per i quali AWS Audit Manager offre un framework e controlli predefiniti. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa in base ai controlli definiti nel AWS Well-Architected Framework. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	44	290	6

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle origini dati in questo framework standard, scarica il file AuditManager_ ConfigDataSourceMappings _AWS-Well-Architected-Framework-WAF-v10.zip.

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi. Inoltre, non possono garantire il superamento dell'audit.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Well-Architected
- AWS Documentazione Well-Architected Framework

Controllo CCCS Medium Cloud

AWS Audit Manager fornisce un framework standard predefinito che supporta il Canadian Centre for Cyber Security (CCCS) Medium Cloud Control.

Argomenti

- Cos'è il CCCS?
- Utilizzo di questo framework
- Passaggi successivi

Cos'è il CCCS?

Il CCCS è l'autorevole fonte canadese di orientamento, servizi e supporto di esperti di sicurezza informatica. Il CCCS fornisce questa esperienza ai governi canadesi, all'industria e al pubblico in generale. Le organizzazioni del settore pubblico canadese dell'intero paese si basano sulle loro rigorose valutazioni dei fornitori di servizi cloud per prendere decisioni informate sugli acquisti cloud.

Il CCCS Medium Cloud Control Profile ha sostituito il profilo PROTECTED B/Medium Integrity/ Medium Availability (PBMM) del governo canadese a maggio 2020. Il CCCS Medium Cloud Security Control Profile è adatto se l'organizzazione utilizza servizi di cloud pubblico per supportare attività aziendali con requisiti medi di riservatezza, integrità e disponibilità (AIC). Per carichi di lavoro con requisiti AIC medi, ci si può ragionevolmente aspettare che la divulgazione, la modifica o la perdita di accesso non autorizzate alle informazioni o ai servizi utilizzati dall'attività aziendale causino gravi danni a un individuo o a un'organizzazione o danni limitati a un gruppo di individui. Ecco alcuni esempi di questi livelli di danni:

- Effetto significativo sull'utile annuo
- Perdita di conti importanti
- Perdita di buona volontà
- Chiara violazione della conformità
- Violazione della privacy per centinaia o migliaia di persone
- Compromissione delle prestazioni del programma
- Disturbi o malattie mentali
- Sabotaggio
- Danni alla reputazione
- Difficoltà finanziarie individuali

Utilizzo di questo framework

Puoi utilizzare il AWS Audit Manager framework per CCCS Medium Cloud Control per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti CCCS. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Audit Manager e iniziare a raccogliere prove rilevanti per un audit di CCCS Medium Cloud Control. Nella valutazione, puoi specificare Account AWS ciò che desideri includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework CCCS Medium Cloud Control. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione.

Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Medium Cloud Control del Canadian Centre for Cyber Security (CCCS)	258	95	175

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file AuditManager_ _ AuditManager _CCCS-Medium-Cloud-Control.zip. ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i tuoi sistemi sono conformi ai requisiti di CCCS Medium Cloud Control. Inoltre, non possono garantire che supererai un audit CCCS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

CIS AWS Benchmark v1.2.0

AWS Audit Manager fornisce due framework predefiniti che supportano il Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0.

> **Note**
>
> - Per informazioni sui framework Gestione audit che supportano la versione 1.3.0, consulta Benchmark AWS CIS v1.3.0.
> - Per informazioni sui framework Gestione audit che supportano la versione 1.4.0, consulta AWS CIS Benchmark v1.4.0.

Argomenti

Cos'è il CIS?

Il CIS è un'organizzazione no profit che ha sviluppato il CIS Foundations Benchmark. AWS Questo benchmark funge da insieme di best practice per la configurazione della sicurezza per. AWS Queste best practice accettate dal settore vanno oltre le linee guida di alto livello in materia di sicurezza già disponibili, step-by-step in quanto forniscono procedure chiare di implementazione e valutazione.

Per ulteriori informazioni, consultate i post del blog CIS AWS Foundations Benchmark sul Security Blog.AWS

Differenza tra i benchmark CIS e i controlli CIS

I benchmark CIS sono linee guida sulle best practice di sicurezza specifiche per i prodotti dei fornitori. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, le impostazioni applicate da un benchmark proteggono i sistemi specifici utilizzati dall'organizzazione. I controlli CIS sono linee guida di best practice fondamentali per i sistemi a livello di organizzazione da seguire per la protezione dai vettori di attacchi informatici noti.

Esempi

- I benchmark CIS sono prescrittivi. In genere fanno riferimento a un'impostazione specifica che può essere rivista e impostata nel prodotto del fornitore.

  Esempio: CIS AWS Benchmark v1.2.0 - Assicurati che l'MFA sia abilitata per l'account «utente root».

  Questa raccomandazione fornisce indicazioni prescrittive su come verificarlo e su come impostarlo sull'account root dell'ambiente. AWS
- I controlli CIS sono rivolti all'intera organizzazione. Non sono specifici per un solo prodotto del fornitore.

  Esempio: CIS v7.1: utilizzo dell'autenticazione a più fattori per tutti gli accessi amministrativi

  Questo controllo descrive cosa dovrebbe essere applicato all'interno dell'organizzazione. Non descrive come applicarlo ai sistemi e ai carichi di lavoro in esecuzione (indipendentemente da dove si trovino).

Utilizzo di questo framework

È possibile utilizzare i framework CIS AWS Benchmark v1.2 per prepararsi agli audit CIS. AWS Audit Manager Puoi inoltre personalizzare questi framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando i framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework CIS. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, livello 1	35	1	4
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, livello 1 e 2	48	1	4

> **Tip**
>
> Per esaminare un elenco delle AWS Config regole utilizzate come mappature delle sorgenti dati per questi framework standard, scarica i seguenti file:
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1-and-2.zip

I controlli in questi framework non hanno lo scopo di verificare se i sistemi sono conformi alle migliori pratiche di CIS Benchmark. AWS Inoltre, non possono garantire che supererai un audit CIS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questi framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Prerequisiti per l'utilizzo di questi framework

Molti controlli nei framework CIS AWS Benchmark v1.2 vengono utilizzati come tipo di origine dati. AWS Config Per supportare questi controlli, è necessario abilitarli AWS Config su tutti gli account in ciascuno dei Regione AWS quali è stato abilitato Audit Manager. È inoltre necessario assicurarsi che siano abilitate AWS Config regole specifiche e che tali regole siano configurate correttamente.

Le seguenti AWS Config regole e parametri sono necessari per raccogliere le prove corrette e acquisire uno stato di conformità accurato per il CIS AWS Foundations Benchmark v1.2. Per istruzioni su come abilitare o configurare una regola, consulta Lavorare con regole gestite AWS Config.

AWS Config Regola obbligatoria	Parametri obbligatori
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • Il numero massimo di giorni senza rotazione. • Tipo: Int • Impostazione predefinita: 90 • Requisito di conformità: un massimo di 90 giorni
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Non applicabile
CLOUD_TRAIL_ENCRYPTION_ENABLED	Non applicabile
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Non applicabile
CMK_BACKING_KEY_ROTATION_ENABLED	Non applicabile
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (facoltativo). • Numero di giorni prima della scadenza della password. • Tipo: int • Impostazione predefinita: 90 • Requisito di conformità: un massimo di 90 giorni
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (facoltativo). • La lunghezza minima della password. • Tipo: int • Impostazione predefinita: 14

AWS Config Regola obbligatoria	Parametri obbligatori
	• Requisito di conformità: minimo 14 caratteri
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (facoltativo). • Numero di password prima di permettere il riutilizzo. • Tipo: int • Impostazione predefinita: 24 • Requisito di conformità: un minimo di 24 password prima del riutilizzo
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (facoltativo). • La password deve contenere almeno un carattere minuscolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un carattere minuscolo
IAM_PASSWORD_POLICY	**`RequireNumbers`** (facoltativo). • La password deve contenere almeno un numero. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un numero
IAM_PASSWORD_POLICY	**`RequireSymbols`** (facoltativo). • La password deve contenere almeno un simbolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un simbolo

AWS Config Regola obbligatoria	Parametri obbligatori
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (facoltativo). • La password deve contenere almeno un carattere maiuscolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un carattere maiuscolo
IAM_POLICY_IN_USE	**`policyARN`** • Un ARN della policy IAM da verificare. • -Tipo: stringa • Requisito di conformità: crea un ruolo IAM per la gestione degli incidenti con AWS. **`policyUsageType`** (facoltativo). • Specifica se si prevede che la policy venga collegata a un utente, un gruppo o un ruolo. • -Tipo: stringa • Valori validi: `IAM_USER`| `IAM_GROUP` | `IAM_ROLE`| `ANY` • Valore predefinito: `ANY` • Requisito di conformità: allega la policy di fiducia al ruolo IAM creato
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Non applicabile
IAM_ROOT_ACCESS_KEY_CHECK	Non applicabile
IAM_USER_NO_POLICIES_CHECK	Non applicabile

AWS Config Regola obbligatoria	Parametri obbligatori
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • Il numero massimo di giorni per i quali una credenziale non può essere utilizzata. • Tipo: Int • Impostazione predefinita: 90 • Requisito di conformità: 90 giorni o più
INCOMING_SSH_DISABLED	Non applicabile
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Non applicabile
MULTI_REGION_CLOUD_TRAIL_ENABLED	Non applicabile

AWS Config Regola obbligatoria	Parametri obbligatori
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (facoltativo). • Numero di porta TCP bloccata. • Tipo: int • Impostazione predefinita: 20 • Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate **`blockedPort2`** (facoltativo). • Numero di porta TCP bloccata. • Tipo: int • Impostazione predefinita: 21 • Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate **`blockedPort3`** (facoltativo). • Numero di porta TCP bloccata. • Tipo: int • Impostazione predefinita: 3389 • Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate **`blockedPort4`** (facoltativo). • Numero di porta TCP bloccata. • Tipo: int • Impostazione predefinita: 3306 • Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate **`blockedPort5`** (facoltativo). • Numero di porta TCP bloccata. • Tipo: int • Impostazione predefinita: 4333

AWS Config Regola obbligatoria	Parametri obbligatori
	• Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Non applicabile
ROOT_ACCOUNT_MFA_ENABLED	Non applicabile
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (facoltativo). • Il bucket S3 di destinazione per l'archiviazione dei log di accesso al server. • -Tipo: stringa • Requisito di conformità: abilita il log **`targetPrefix`** (facoltativo). • Il prefisso del bucket S3 per l'archiviazione dei log di accesso al server. • -Tipo: stringa • Requisito di conformità: identifica il bucket S3 per la registrazione CloudTrail
S3_BUCKET_PUBLIC_READ_PROHIBITED	Non applicabile
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Non applicabile
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (facoltativo). • Il `trafficType` dei log di flusso. • -Tipo: stringa • Requisito di conformità: il log del flusso è abilitato

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Il benchmark CIS Foundations v1.2.0 AWS
- Post del blog di CIS AWS Foundations Benchmark sul Blog sulla sicurezza AWS

Benchmark AWS CIS v1.3.0

AWS Audit Manager fornisce due framework standard predefiniti che supportano CIS Benchmark v1.3. AWS

> **Note**
>
> - Per informazioni sui framework Gestione audit che supportano la versione 1.2.0, consulta CIS AWS Benchmark v1.2.0.
> - Per informazioni sui framework Gestione audit che supportano la versione 1.4.0, consulta AWS CIS Benchmark v1.4.0.

Argomenti

Cos'è il CIS Benchmark? AWS

Il CIS ha sviluppato il CIS AWS Foundations Benchmark v1.3.0, un insieme di best practice per la configurazione della sicurezza. AWS Queste best practice accettate dal settore vanno oltre le linee guida di alto livello in materia di sicurezza già disponibili, in quanto forniscono AWS agli utenti procedure chiare di implementazione e valutazione. step-by-step

Per ulteriori informazioni, consultate i post del blog CIS AWS Foundations Benchmark sul Security Blog.AWS

CIS AWS Benchmark v1.3.0 fornisce indicazioni per la configurazione delle opzioni di sicurezza per un sottoinsieme di, Servizi AWS con particolare attenzione alle impostazioni di base, testabili e indipendenti dall'architettura. Ecco alcuni degli Amazon Web Services specifici nell'ambito di applicazione del presente documento:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (predefinito)

Differenza tra i benchmark CIS e i controlli CIS

I benchmark CIS sono linee guida sulle best practice di sicurezza specifiche per i prodotti dei fornitori. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, le impostazioni applicate da un benchmark proteggono i sistemi utilizzati dall'organizzazione. I controlli CIS sono linee guida fondamentali sulle best practice che l'organizzazione deve seguire per la protezione dai vettori di attacco informatico noti.

Esempi

- I benchmark CIS sono prescrittivi. In genere fanno riferimento a un'impostazione specifica che può essere rivista e impostata nel prodotto del fornitore.

  Esempio: CIS AWS Benchmark v1.3.0 - Assicurarsi che l'MFA sia abilitata per l'account «utente root»

Questa raccomandazione fornisce indicazioni prescrittive su come verificarlo e su come impostarlo sull'account root dell'ambiente. AWS

- I controlli CIS sono rivolti all'intera organizzazione e non sono specifici per un solo prodotto del fornitore.

  Esempio: CIS v7.1: utilizzo dell'autenticazione a più fattori per tutti gli accessi amministrativi

  Questo controllo descrive cosa dovrebbe essere applicato all'interno dell'organizzazione, ma non come applicarlo ai sistemi e ai carichi di lavoro in esecuzione (indipendentemente da dove si trovino).

Utilizzo di questi framework

È possibile utilizzare i framework CIS AWS Benchmark v1.3 per prepararsi agli audit CIS. AWS Audit Manager Puoi inoltre personalizzare questi framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando i framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework CIS. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, livello 1	36	1	5

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, livello 1 e 2	54	1	5

> **Tip**
>
> Per esaminare un elenco delle AWS Config regole utilizzate come mappature delle sorgenti dati per questi framework standard, scarica i seguenti file:
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1-and-2.zip

I controlli in questi framework non hanno lo scopo di verificare se i sistemi sono conformi alle migliori pratiche di CIS Benchmark. AWS Inoltre, non possono garantire che supererai un audit CIS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questi framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Post del blog di CIS AWS Foundations Benchmark sul Blog sulla sicurezza AWS

AWS CIS Benchmark v1.4.0

AWS Audit Manager fornisce due framework standard predefiniti che supportano il Center for Internet Security (CIS) Foundations Benchmark v1.4.0. AWS

> **Note**
>
> - Per informazioni sui framework Gestione audit che supportano la versione 1.2.0, consulta CIS AWS Benchmark v1.2.0.
> - Per informazioni sui framework Gestione audit che supportano la versione 1.3.0, consulta Benchmark AWS CIS v1.3.0.

Argomenti

Cos' AWS è il benchmark CIS?

Il CIS AWS Benchmark v1.4.0 fornisce linee guida prescrittive per la configurazione delle opzioni di sicurezza per un sottoinsieme di Amazon Web Services. Pone l'accento sulle impostazioni fondamentali, testabili e indipendenti dall'architettura. Ecco alcuni degli Amazon Web Services specifici nell'ambito di applicazione del presente documento:

- AWS Identity and Access Management (IAM)
- Sistema di analisi degli accessi AWS IAM
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))
- Amazon Simple Storage Service (Amazon S3)

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Differenza tra i benchmark CIS e i controlli CIS

I benchmark CIS sono linee guida sulle best practice di sicurezza specifiche per i prodotti dei fornitori. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, le impostazioni applicate da un benchmark proteggono i sistemi utilizzati. I controlli CIS sono linee guida fondamentali sulle best practice che l'organizzazione deve seguire per la protezione dai vettori di attacco informatico noti.

Esempi

- I benchmark CIS sono prescrittivi. In genere fanno riferimento a un'impostazione specifica che può essere rivista e impostata nel prodotto del fornitore.

  Esempio: CIS AWS Benchmark v1.3.0 - Assicurarsi che l'MFA sia abilitata per l'account «utente root»

  Questa raccomandazione fornisce indicazioni prescrittive su come verificarlo e su come impostarlo sull'account root dell'ambiente. AWS
- I controlli CIS sono rivolti all'intera organizzazione e non sono specifici per un solo prodotto del fornitore.

  Esempio: CIS v7.1: utilizzo dell'autenticazione a più fattori per tutti gli accessi amministrativi

  Questo controllo descrive cosa dovrebbe essere applicato all'interno dell'organizzazione. Tuttavia, non descrive come applicarlo ai sistemi e ai carichi di lavoro in esecuzione, indipendentemente da dove si trovino.

Utilizzo di questi framework a supporto della preparazione dell'audit

È possibile utilizzare i framework CIS AWS Benchmark v1.4.0 per prepararsi agli audit CIS. AWS Audit Manager Puoi inoltre personalizzare questi framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando i framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a

valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework CIS. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, livello 1	37	1	5
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, livello 1 e 2	57	1	5

> **Tip**
>
> Per esaminare un elenco delle AWS Config regole utilizzate come mappature delle sorgenti dati per questi framework standard, scarica i seguenti file:
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1-and-2.zip

I controlli in questi framework non hanno lo scopo di verificare se i sistemi sono conformi al CIS Benchmark v1.4.0. AWS Inoltre, non possono garantire che supererai un audit CIS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questi framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Benchmark CIS del Center for Internet Security
- Post del blog di CIS AWS Foundations Benchmark sul Blog sulla sicurezza AWS

Controlli CIS v7.1, IG1

AWS Audit Manager fornisce un framework standard predefinito che supporta Center for Internet Security (CIS) v7.1 Implementation Group 1.

> **Note**
>
> Per informazioni su CIS v8 IG1 e sul framework che supporta questo standard, vedere. AWS Audit Manager CIS Critical Security Controls versione 8.0, IG1

Argomenti

Cosa sono i controlli CIS?

I controlli CIS sono un insieme di azioni prioritarie che, collettivamente, costituiscono un insieme di best practice. defense-in-depth Queste best practice mitigano gli attacchi più comuni contro sistemi e

reti. Generalmente, per un'organizzazione con risorse limitate e competenze di sicurezza informatica disponibili per implementare i controlli secondari, viene definito il gruppo di implementazione 1.

Differenza tra i controlli CIS e i benchmark CIS

I controlli CIS sono linee guida fondamentali sulle best practice che un'organizzazione può seguire per proteggersi dai vettori di attacchi informatici noti. I benchmark CIS sono linee guida sulle best practice di sicurezza specifiche per i prodotti dei fornitori. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, le impostazioni applicate da un benchmark proteggono i sistemi utilizzati.

Esempi

- I benchmark CIS sono prescrittivi. In genere fanno riferimento a un'impostazione specifica che può essere rivista e impostata nel prodotto del fornitore.
  - Esempio: CIS AWS Benchmark v1.2.0 - Assicurarsi che l'MFA sia abilitata per l'account «utente root»
  - Questa raccomandazione fornisce indicazioni prescrittive su come verificarlo e su come impostarlo sull'account root dell'ambiente. AWS
- I controlli CIS sono rivolti all'intera organizzazione e non sono specifici per un solo prodotto del fornitore.
  - Esempio: CIS v7.1: utilizzo dell'autenticazione a più fattori per tutti gli accessi amministrativi
  - Questo controllo descrive cosa dovrebbe essere applicato all'interno dell'organizzazione. Tuttavia, non descrive come applicarlo ai sistemi e ai carichi di lavoro in esecuzione (indipendentemente da dove si trovino).

Utilizzo di questo framework

Puoi utilizzare il framework Controlli CIS v7.1 IG1 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti CIS. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework CIS Controls v7.1 IG1. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle

delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework CIS Controls v7.1 IG1 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Center for Internet Security (CIS) v7.1, IG1	31	12	18

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file _ _CIS-v7.1-ig1.zip. AuditManager ConfigDataSourceMappings

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi ai controlli CIS. Inoltre, non possono garantire il superamento di un audit CIS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Controlli CIS v7.1 IG1

CIS Critical Security Controls versione 8.0, IG1

AWS Audit Manager fornisce un framework standard predefinito che supporta la versione 8.0 di CIS Critical Security Controls, Implementation Group 1.

> **Note**
>
> Per informazioni su CIS v7.1, IG1 e sul AWS Audit Manager framework che supporta questo standard, vedere. Controlli CIS v7.1, IG1

Argomenti

Cosa sono i controlli CIS?

I controlli CIS Critical Security Controls (controlli CIS) sono un insieme di misure di sicurezza prioritarie per la mitigazione degli attacchi informatici più diffusi contro sistemi e reti. Sono mappati e referenziati da diversi framework legali, normativi e politici. CIS Controls v8 è stato migliorato per stare al passo con i sistemi e i software moderni. Il passaggio all'elaborazione basata sul cloud, alla virtualizzazione, alla mobilità, all'outsourcing e al cambiamento delle tattiche degli aggressori ha portato all'aggiornamento work-from-home. Questo aggiornamento supporta la sicurezza delle aziende che passano ad ambienti completamente cloud e ibridi.

Differenza tra i controlli CIS e i benchmark CIS

I controlli CIS sono linee guida fondamentali sulle best practice che un'organizzazione può seguire per proteggersi dai vettori di attacchi informatici noti. I benchmark CIS sono linee guida sulle best practice di sicurezza specifiche per i prodotti dei fornitori. Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, le impostazioni applicate da un benchmark proteggono i sistemi utilizzati.

Esempi

- I benchmark CIS sono prescrittivi. In genere fanno riferimento a un'impostazione specifica che può essere rivista e impostata nel prodotto del fornitore.
  - Esempio: CIS AWS Benchmark v1.2.0 - Assicurarsi che l'MFA sia abilitata per l'account «utente root»
  - Questa raccomandazione fornisce indicazioni prescrittive su come verificarlo e su come impostarlo sull'account root dell'ambiente. AWS
- I controlli CIS sono rivolti all'intera organizzazione e non sono specifici per un solo prodotto del fornitore.
  - Esempio: CIS v7.1: utilizzo dell'autenticazione a più fattori per tutti gli accessi amministrativi
  - Questo controllo descrive cosa dovrebbe essere applicato all'interno dell'organizzazione. Tuttavia, non descrive come applicarlo ai sistemi e ai carichi di lavoro in esecuzione (indipendentemente da dove si trovino).

Utilizzo di questo framework

È possibile utilizzare il framework CIS v8 IG1 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti CIS. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework CIS v8. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
CIS Critical Security Controls versione 8.0 (CIS v8.0), IG1	38	18	15

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file _ _CIS-v8.0-ig1.zip. AuditManager ConfigDataSourceMappings

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi ai controlli CIS. Inoltre, non possono garantire il superamento di un audit CIS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- CIS Controls v8

FedRAMP Security Baseline Controls r4

AWS Audit Manager fornisce un framework standard predefinito che supporta il Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4.

Argomenti

Cos'è FedRAMP?

FedRAMP è stata fondata nel 2011. Fornisce un approccio economico e basato sul rischio per l'adozione e l'uso dei servizi cloud da parte del governo federale degli Stati Uniti. FedRAMP consente alle agenzie federali di utilizzare moderne tecnologie cloud, con particolare attenzione alla sicurezza e alla protezione delle informazioni federali.

Per ulteriori informazioni sui controlli di base moderati di FedRAMP, consulta il modello delle procedure per i test di sicurezza moderati di FedRAMP.

Utilizzo di questo framework

È possibile utilizzare il framework FedRAMP r4 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controllo in base ai requisiti FedRAMP r4. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework FedRAMP Moderate Baseline sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Controlli di base sulla sicurezza del Federal Risk and Authorization Management Program (FedRAMP) r4, Moderate	234	91	17

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il ConfigDataSourceMappingsfile AuditManager _ _FedRAMP-Security-Baseline-Controls-r4-Moderate.zip.

I controlli in questo framework non hanno lo scopo di verificare se i sistemi sono conformi a FedRAMP r4. Inoltre, non possono garantire il superamento di un audit FedRAMP. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Pagina di conformità per FedRAMP
- AWS Post del blog FedRAMP

GDPR 2016

AWS Audit Manager fornisce un framework standard predefinito che supporta il Regolamento generale sulla protezione dei dati (GDPR) 2016.

Questo framework contiene solo controlli manuali. Questi controlli manuali non raccolgono prove in modo automatico. Tuttavia, se desideri automatizzare la raccolta delle prove per alcuni controlli previsti dal GDPR, puoi utilizzare la funzionalità di controllo personalizzata in Audit Manager. Per ulteriori informazioni, consulta Utilizzo di questo framework.

Argomenti

Cos'è il GDPR?

Il GDPR è una legge europea sulla privacy che è entrata in vigore il 25 maggio 2018. Il GDPR sostituisce la Direttiva sulla protezione dei dati dell'UE, nota anche come Direttiva 95/46/CE. Ha lo scopo di armonizzare le leggi sulla protezione dei dati in tutta l'Unione europea (UE). Lo fa applicando un'unica legge sulla protezione dei dati vincolante in ogni stato membro dell'UE.

Il GDPR si applica a tutte le organizzazioni con sede nell'UE e alle organizzazioni (indipendentemente dal fatto che siano state costituite nell'UE) che trattano i dati personali degli interessati dell'UE in relazione all'offerta di beni o servizi ai soggetti interessati nell'UE o al monitoraggio del comportamento che ha luogo all'interno dell'UE. Per dati personali si intendono tutte le informazioni relative a una persona fisica identificata o identificabile.

Puoi trovare il framework GDPR nella pagina della libreria del framework di Audit Manager. Per ulteriori informazioni, consulta il Centro generale sulla protezione dei dati (GDPR).

Utilizzo di questo framework

Puoi utilizzare il framework GDPR 2016 in Audit Manager per prepararti agli audit.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Regolamento generale sulla protezione dei dati (GDPR) 2016	0	378	10

Puoi trovare il framework GDPR 2016 nella scheda Standard frameworks di Audit Utilizzo della libreria di framework per gestire i framework in AWS Audit Manager Manager. Questo framework standard contiene solo controlli manuali.

> **Note**
>
> Se desideri automatizzare la raccolta di prove per il GDPR, puoi utilizzare Gestione audit per creare controlli personalizzati per il GDPR. La tabella seguente fornisce consigli sulle fonti di AWS dati che puoi mappare ai requisiti del GDPR nei tuoi controlli personalizzati. Sebbene alcune delle seguenti origini dati siano mappate su più controlli, tieni presente che ti viene addebitato un solo importo per ogni valutazione delle risorse.
> I seguenti consigli utilizzano AWS Config e AWS Security Hub come fonti di dati. Per raccogliere con successo prove da queste fonti di dati, assicurati di aver seguito le istruzioni per abilitare e configurare AWS Config e inserire AWS Security Hub nel tuo Account AWS. Dopo aver configurato entrambi i servizi in questo modo, Audit Manager raccoglie le prove ogni volta che viene effettuata una valutazione per la AWS Config regola specificata o il controllo del Security Hub.

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 25 Protezione dei dati fin dalla progettazione e per	Capitolo 4 - Titolare e responsabile del	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
impostazione predefinita.1	trattamento	• AWS CloudTrail bucket non pubblico • Mostra tutte le policy con un `Allow:*:*` ed elenca tutti i principali e i servizi che utilizzano tali policy Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (.10) CloudWatch • 3.11 (.11) CloudWatch • 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita.2	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale • AWS CloudTrail bucket non pubblico • Mostra tutte le policy con un `Allow:*:*` ed elenca tutti i principali e i servizi che utilizzano tali policy Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (.10) CloudWatch • 3.11 (.11) CloudWatch • 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita.3	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale • AWS CloudTrail bucket non pubblico • Mostra tutte le policy con un `Allow:*:*` ed elenca tutti i principali e i servizi che utilizzano tali policy Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (.10) CloudWatch • 3.11 (.11) CloudWatch • 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• Config.1
Articolo 30 Registrazione delle attività di trattamento.1	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo Security Hub come mappatura dell'origine dati: • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 30 Registrazione delle attività di trattamento.2	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo Security Hub come mappatura dell'origine dati: • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 30 Registrazione delle attività di trattamento.3	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale • AWS CloudTrail bucket non pubblico • Mostra tutte le policy con un `Allow:*:*` ed elenca tutti i principali e i servizi che utilizzano tali policy Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo Security Hub come mappatura dell'origine dati: • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 30 Registrazione delle attività di trattamento.4	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale • AWS CloudTrail bucket non pubblico • Mostra tutte le policy con un `Allow:*:*` ed elenca tutti i principali e i servizi che utilizzano tali policy Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo Security Hub come mappatura dell'origine dati: • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 30 Registrazione delle attività di trattamento.5	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra tutti gli eventi dell'account root in un arco temporale Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo Security Hub come mappatura dell'origine dati: • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 32 Sicurezza del trattamento.1	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra la crittografia dei dati a riposo per tutti i servizi • Mostra la crittografia dei dati in transito per tutti i servizi • MFA Delete abilitato per Amazon S3 • Tutte le scansioni di Amazon Inspector • Mostra tutte le istanze che non sono abilitate ad Amazon Inspector • Mostra tutti i sistemi di bilanciamento del carico in ascolto su HTTPS (SSL) • AWS CloudTrail crittografato a riposo • CloudWatch Avvisi Amazon per la AWS Config visualizzazione di tutte le modifiche e di tutte le impostazioni commentate • Tutte le attività root Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 32 Sicurezza del trattamento.2	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra la crittografia dei dati a riposo per tutti i servizi • Mostra la crittografia dei dati in transito per tutti i servizi • MFA Delete abilitato per Amazon S3 • Tutte le scansioni di Amazon Inspector • Mostra tutte le istanze che non sono abilitate ad Amazon Inspector • Mostra tutti i sistemi di bilanciamento del carico in ascolto su HTTPS (SSL) • AWS CloudTrail crittografato a riposo • CloudWatch Avvisi Amazon per la AWS Config visualizzazione di tutte le modifiche e di tutte le impostazioni commentate • Tutte le attività root Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 32 Sicurezza del trattamento.3	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra la crittografia dei dati a riposo per tutti i servizi • Mostra la crittografia dei dati in transito per tutti i servizi • MFA Delete abilitato per Amazon S3 • Tutte le scansioni di Amazon Inspector • Mostra tutte le istanze che non sono abilitate ad Amazon Inspector • Mostra tutti i sistemi di bilanciamento del carico in ascolto su HTTPS (SSL) • AWS CloudTrail crittografato a riposo • CloudWatch Avvisi Amazon per la AWS Config visualizzazione di tutte le modifiche e di tutte le impostazioni commentate • Tutte le attività root Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 32 Sicurezza del trattamento.4	Capitolo 4 - Titolare e responsabile del trattamento	Puoi creare un controllo personalizzato AWS Audit Manager che supporti questo controllo GDPR. Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test: • Mostra la crittografia dei dati a riposo per tutti i servizi • Mostra la crittografia dei dati in transito per tutti i servizi • MFA Delete abilitato per Amazon S3 • Tutte le scansioni di Amazon Inspector • Mostra tutte le istanze che non sono abilitate ad Amazon Inspector • Mostra tutti i sistemi di bilanciamento del carico in ascolto su HTTPS (SSL) • AWS CloudTrail crittografato a riposo • CloudWatch Avvisi Amazon per la AWS Config visualizzazione di tutte le modifiche e di tutte le impostazioni commentate • Tutte le attività root Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati: Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole AWS Config gestite come mappature delle origini dati: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Dopo aver creato i nuovi controlli personalizzati per il GDPR, puoi aggiungerli a un framework GDPR personalizzato. È possibile creare una valutazione dal framework GDPR personalizzato. In questo modo, Audit Manager può raccogliere automaticamente le prove per i controlli personalizzati che hai aggiunto.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consultaCreazione di una copia modificabile di un framework esistente in AWS Audit Manager.

Risorse aggiuntive

- Centro per il Regolamento generale sulla protezione dei dati (GDPR)
- AWS Post del blog sul GDPR

Gramm-Leach-Bliley Act

AWS Audit Manager fornisce un framework predefinito che supporta il Gramm-Leach-Bliley Act (GLBA).

Argomenti

Cos'è il GLBA?

Il GLBA (o GLB Act), noto anche come Financial Service Modernization Act del 1999, è una legge federale emanata negli Stati Uniti per controllare il modo in cui gli istituti finanziari trattano le informazioni private delle persone. La legge è costituita da tre sezioni. La prima è la Financial Privacy Rule, che regola la raccolta e la divulgazione di informazioni finanziarie private. La seconda è la Safeguards Rule, che stabilisce che gli istituti finanziari devono implementare programmi di sicurezza per la protezione di tali informazioni. La terza riguarda le disposizioni relative al pretexting, che vietano la pratica del pretexting (accesso a informazioni private utilizzando falsi pretesti). La legge impone inoltre agli istituti finanziari di fornire ai clienti avvisi scritti sulla privacy che spieghino le loro pratiche di condivisione delle informazioni.

Utilizzo di questo framework

È possibile utilizzare il framework GLBA 2016 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti GLBA. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework GLBA come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per un audit GLBA. Nella valutazione, è possibile specificare Account AWS ciò che si desidera includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework GLBA. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Gramm-Leach-Bliley Act (GLBA)	0	120	16

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard GLBA. Inoltre, non possono garantire che supererai un audit GLBA. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare il framework GLBA nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Titolo 21 CFR, parte 11

AWS Audit Manager fornisce un framework standard predefinito che supporta il Titolo 21 del Codice dei regolamenti federali (CFR), parte 11, Record elettronici; firme elettroniche - Ambito di applicazione e applicazione il 24 maggio 2023.

Argomenti

Cos'è il Titolo 21 della Parte 11 del CFR?

GxP fa riferimento ai regolamenti e alle linee guida applicabili alle organizzazioni delle scienze della vita che producono prodotti alimentari e medici. I prodotti medici che rientrano in questa categoria includono medicinali, dispositivi medici e applicazioni software mediche. L'intento generale dei requisiti GxP è garantire che i prodotti alimentari e medici siano sicuri per i consumatori. Serve anche a garantire l'integrità dei dati utilizzati per prendere decisioni sulla sicurezza relative ai prodotti.

Negli Stati Uniti, le normative GxP sono applicate dalla Food and Drug Administration (FDA) statunitense e sono contenute nel Titolo 21 del Codice dei regolamenti federali (21 CFR). All'interno del 21 CFR, la Parte 11 contiene i requisiti per i sistemi informatici che creano, modificano, mantengono, archiviano, recuperano o distribuiscono record elettronici e firme elettroniche a supporto delle attività regolate dalla GxP. La Parte 11 è stata creata per consentire l'adozione di nuove tecnologie informatiche da parte delle organizzazioni di scienze della vita regolamentate dalla FDA, fornendo allo stesso tempo un quadro per garantire che i dati elettronici GxP siano affidabili e affidabili.

Per un approccio completo all'utilizzo del AWS Cloud per i sistemi GxP, consulta il white paper Considerazioni sull'utilizzo AWS dei prodotti nei sistemi GxP.

Utilizzo di questo framework

Puoi utilizzare il framework Title 21 CFR Part 11 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controllo in base ai requisiti CFR. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel quadro del Titolo 21 CFR Part 11. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Titolo 21 Codice dei regolamenti federali (CFR), parte 11, Registri elettronici; firme elettroniche -	17	8	2

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Ambito di applicazione e applicazione 24 maggio 2023			

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il AuditManager file _ _Title-21-CFR-Part-11.zip. ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi alle normative GxP. Inoltre, non possono garantire il superamento di un audit. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Pagina di conformità per GxP
- Considerazioni sull'utilizzo dei AWS prodotti nei sistemi GxP

Allegato 11, v1, GMP dell'UE

AWS Audit Manager fornisce un quadro predefinito che supporta le EudraLex - Le norme che disciplinano i medicinali nell'Unione europea (UE) - Volume 4: Good Manufacturing Practice (GMP) dei medicinali per uso umano e veterinario - Allegato 11.

Argomenti

Cos'è l'allegato 11 delle GMP dell'UE?

Il quadro GMP dell'allegato 11 dell'UE è l'equivalente europeo del quadro normativo relativo al Titolo 21 del CFR, parte 11 negli Stati Uniti. Questo allegato si applica a tutte le forme di sistemi computerizzati utilizzati nell'ambito delle attività regolamentate dalle buone prassi di fabbricazione (GMP). Un sistema computerizzato è un insieme di componenti software e hardware che insieme soddisfano determinate funzionalità. L'applicazione deve essere convalidata e l'infrastruttura IT deve essere qualificata. Laddove un sistema computerizzato sostituisce un funzionamento manuale, non dovrebbe verificarsi alcuna riduzione della qualità del prodotto, del controllo del processo o della garanzia della qualità. Non dovrebbe esserci alcun aumento del rischio complessivo del processo.

L'allegato 11 fa parte delle linee guida europee GMP e definisce i termini di riferimento per i sistemi computerizzati utilizzati dalle organizzazioni dell'industria farmaceutica. L'allegato 11 funge da lista di controllo che consente alle agenzie di regolamentazione europee di stabilire i requisiti per i sistemi computerizzati relativi a prodotti farmaceutici e dispositivi medici. Le linee guida stabilite dalla Commissione dei comitati europei non sono molto lontane dalla FDA (Titolo 21 CFR Parte 11). L'allegato 11 definisce i criteri per la gestione dei record elettronici e delle firme elettroniche.

Utilizzo di questo framework

Puoi utilizzare il framework UE GMP Annex 11 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti GMP dell'UE. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel quadro dell'allegato 11 delle GMP dell'UE. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete

esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
EudraLex - Le norme che disciplinano i medicinali nell'Unione europea (UE) - Volume 4: Medicinali di buona fabbricazione (GMP) per uso umano e veterinario - Allegato 11	15	17	3

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle fonti di dati in questo framework standard, scaricate il file AuditManager_ _ ConfigDataSourceMappings -GMP-Volume-4-Annex-11.zip. EudraLex

I controlli di questo framework non hanno lo scopo di verificare se i sistemi sono conformi ai requisiti dell'allegato 11 delle GMP dell'UE. Inoltre, non possono garantire che supererai un audit GMP dell'UE. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Regola di sicurezza HIPAA: febbraio 2003

AWS Audit Manager fornisce un framework standard predefinito che supporta la regola di sicurezza dell'Health Insurance Portability and Accountability Act (HIPAA): febbraio 2003.

> **Note**
>
> Per informazioni sulla norma di sicurezza Omnibus finale HIPAA 2013 e sul framework Gestione audit che supporta questo standard, consulta Regola finale HIPAA Omnibus.

Argomenti

Cosa sono l'HIPAA e la norma di sicurezza HIPAA 2003?

L'HIPAA è una legislazione che aiuta i lavoratori statunitensi a mantenere la copertura assicurativa sanitaria in caso di cambio o perdita di lavoro. La legislazione mira inoltre a incoraggiare l'uso delle cartelle cliniche elettroniche per migliorare l'efficienza e la qualità del sistema sanitario statunitense attraverso una migliore condivisione delle informazioni.

Oltre ad aumentare l'uso delle cartelle cliniche elettroniche, l'HIPAA include disposizioni per la protezione della sicurezza e della privacy delle informazioni sanitarie protette (PHI). PHI include una serie molto ampia di dati sanitari e relativi alla salute identificabili personalmente. Tra questi dati figurano informazioni sull'assicurazione e sulla fatturazione, dati di diagnosi, dati sull'assistenza clinica e risultati di laboratorio come immagini e risultati dei test.

Il Dipartimento della Salute e dei Servizi Umani degli Stati Uniti ha pubblicato una norma di sicurezza finale nel febbraio 2003. Questa regola stabilisce gli standard nazionali per la protezione della riservatezza, dell'integrità e della disponibilità di informazioni sanitarie protette in formato elettronico.

Le regole HIPAA si applicano alle entità coinvolte. Tra esse figurano ospedali, fornitori di servizi medici, piani sanitari sponsorizzati dai datori di lavoro, strutture di ricerca e compagnie assicurative che si occupano direttamente dei pazienti e dei dati dei pazienti. Il requisito HIPAA per la protezione dei PHI si estende anche ai partner coinvolti.

Per ulteriori informazioni su come HIPAA e HITECH proteggono le informazioni sanitarie, consulta la pagina web Health Information Privacy del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti.

Un numero crescente di fornitori di servizi sanitari, pagatori e professionisti IT utilizza servizi cloud AWS basati sulle utilità per elaborare, archiviare e trasmettere informazioni sanitarie protette (PHI). AWS consente alle entità coperte e ai loro partner commerciali soggetti all'HIPAA di utilizzare l' AWS ambiente sicuro per elaborare, mantenere e archiviare informazioni sanitarie protette.

Per istruzioni su come utilizzarle AWS per l'elaborazione e l'archiviazione di informazioni sanitarie, consulta il white paper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilizzo di questo framework

Puoi utilizzare il framework della Norma di sicurezza HIPAA 2003 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti HIPAA. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework HIPAA. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Norma di sicurezza dell'Health Insurance Portability and Accountability Act (HIPAA): febbraio 2003	45	40	5

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle origini dati in questo framework standard, scaricate il file _ _HIPAA-Security-Rule-Feb-2003.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard HIPAA. Inoltre, non possono garantire che supererai un audit HIPAA. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Privacy delle informazioni sanitarie del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti
- La norma di sicurezza del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti

- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Pagina di conformità per l'HIPAA

Regola finale HIPAA Omnibus

AWS Audit Manager fornisce un framework standard predefinito che supporta l'Omnibus Final Rule dell'Health Insurance Portability and Accountability Act (HIPAA).

> **Note**
>
> Per informazioni sulla norma di sicurezza HIPAA 2003 e sul AWS Audit Manager framework che supporta questo standard, vedere. Regola di sicurezza HIPAA: febbraio 2003

Argomenti

Cosa sono l'HIPAA e la norma di sicurezza Omnibus finale HIPAA?

L'HIPPA è una legislazione che aiuta i lavoratori statunitensi a mantenere la copertura assicurativa sanitaria quando cambiano o perdono il lavoro. La legislazione mira inoltre a incoraggiare l'uso delle cartelle cliniche elettroniche per migliorare l'efficienza e la qualità del sistema sanitario statunitense attraverso una migliore condivisione delle informazioni.

Oltre ad aumentare l'uso delle cartelle cliniche elettroniche, l'HIPAA include disposizioni per la protezione della sicurezza e della privacy delle informazioni sanitarie protette (PHI). PHI include una serie molto ampia di dati sanitari e relativi alla salute identificabili personalmente. Tra questi dati figurano informazioni sull'assicurazione e sulla fatturazione, dati di diagnosi, dati sull'assistenza clinica e risultati di laboratorio come immagini e risultati dei test.

La norma di sicurezza Omnibus finale HIPAA, entrata in vigore nel 2013, implementa una serie di aggiornamenti a tutte le regole precedentemente approvate. Le modifiche alle norme di sicurezza,

privacy, notifica delle violazioni e applicazione avevano lo scopo di migliorare la riservatezza e la sicurezza nella condivisione dei dati.

Le regole HIPAA si applicano alle entità coinvolte. Tra esse figurano ospedali, fornitori di servizi medici, piani sanitari sponsorizzati dai datori di lavoro, strutture di ricerca e compagnie assicurative che si occupano direttamente dei pazienti e dei dati dei pazienti. Come parte degli aggiornamenti Omnibus, molte delle norme HIPAA che si applicano alle entità coinvolte ora si applicano anche ai partner coinvolti.

Per ulteriori informazioni su come HIPAA e HITECH proteggono le informazioni sanitarie, consulta la pagina web Health Information Privacy del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti.

Un numero crescente di fornitori di servizi sanitari, pagatori e professionisti IT utilizza servizi cloud AWS basati sulle utilità per elaborare, archiviare e trasmettere informazioni sanitarie protette (PHI). AWS consente alle entità coperte e ai loro partner commerciali soggetti all'HIPAA di utilizzare l' AWS ambiente sicuro per elaborare, mantenere e archiviare informazioni sanitarie protette. Per istruzioni su come utilizzarle AWS per l'elaborazione e l'archiviazione di informazioni sanitarie, consulta il white paper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilizzo di questo framework

Puoi utilizzare il framework HIPAA Omnibus Final Rule per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti HIPAA. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework HIPAA. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Regola finale omnibus dell'Health Insurance Portability and Accountability Act (HIPAA)	45	29	5

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle origini dati in questo framework standard, scaricate il file _ _HIPAA-Omnibus-Final-Rule.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard HIPAA. Inoltre, non possono garantire che supererai un audit HIPAA. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Privacy delle informazioni sanitarie del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti
- Regolamentazione Omnibus HIPAA del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti

- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Pagina di conformità per l'HIPAA

ISO/IEC 27001:2013 Allegato A

AWS Audit Manager fornisce un framework standard predefinito che supporta l'Organizzazione internazionale per la standardizzazione (ISO) /Commissione elettrotecnica internazionale (IEC) 27001:2013 Allegato A..

Argomenti

- Che cos'è lo standard ISO/IEC 27001:2013 Allegato A?
- Utilizzo di questo framework
- Passaggi successivi
- Risorse aggiuntive

Che cos'è lo standard ISO/IEC 27001:2013 Allegato A?

La Commissione elettrotecnica internazionale (IEC) e l'Organizzazione internazionale per la standardizzazione (ISO) sono entrambe organizzazioni indipendenti e non governative che sviluppano e pubblicano standard internazionali basati sul pieno consenso. not-for-profit

ISO/IEC 27001:2013 Allegato A è uno standard di gestione della sicurezza che specifica le best practice di gestione della sicurezza e controlli di sicurezza completi che seguono le linee guida sulle best practice ISO/IEC 27002. Questo standard internazionale specifica i requisiti su come stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni all'interno dell'organizzazione. Tra questi standard vi sono requisiti per la valutazione e il trattamento dei rischi per la sicurezza delle informazioni che sono personalizzati in base alle esigenze dell'organizzazione. I requisiti di questo standard internazionale sono generici e sono destinati ad essere applicabili a tutte le organizzazioni, indipendentemente dalla tipologia, dalle dimensioni o dalla natura.

Utilizzo di questo framework

È possibile utilizzare il AWS Audit Manager framework per l'allegato A della norma ISO/IEC 27001:2013 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli

con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controllo secondo i requisiti dello standard ISO/IEC 27001:2013 Allegato A. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per un audit dello standard ISO/IEC 27001:2013 Allegato A. Nella valutazione, è possibile specificare Account AWS ciò che si desidera includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework dello ISO/IEC 27001:2013 Allegato A. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Organizzazione internazionale per la standardizzazione (ISO) /Commissione elettrotecnica internazionale (IEC) 27001:2013 Allegato A	61	53	35

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file _ _ISO-IEC-270012013-Annex-A.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi a questo standard internazionale. Inoltre, non possono garantire che supererai un audit

ISO/IEC. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Puoi trovare il framework dello standard ISO/IEC 27001:2013 Allegato A nella scheda Framework standard della Utilizzo della libreria di framework per gestire i framework in AWS Audit Manager di Gestione audit.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consultaCreazione di una copia modificabile di un framework esistente in AWS Audit Manager.

Risorse aggiuntive

- Per ulteriori informazioni su questo standard internazionale, consulta ISO/IEC 27001:2013 sull'ANSI Webstore.

NIST SP 800-53 Rev. 5

AWS Audit Manager fornisce un framework predefinito che supporta il NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations.

> **Note**
>
> - Per informazioni sul framework Audit Manager che supporta NIST SP 800-171, vedere. NIST SP 800-171 Rev. 2
> - Per informazioni sul framework Audit Manager che supporta NIST CSF, vedere. NIST Cybersecurity Framework v1.1

Argomenti

- Risorse aggiuntive

Cos'è NIST SP 800-53?

Il National Institute of Standards and Technology (NIST) è stato fondato nel 1901 e ora fa parte del Dipartimento del Commercio degli Stati Uniti. Il NIST è uno dei più antichi laboratori di scienze fisiche degli Stati Uniti. Il Congresso degli Stati Uniti istituì l'agenzia per migliorare quella che all'epoca era un'infrastruttura di misurazione di seconda categoria. L'infrastruttura rappresentava una sfida importante per la competitività industriale degli Stati Uniti, essendo rimasta indietro rispetto ad altre potenze economiche come il Regno Unito e la Germania.

I controlli di sicurezza NIST SP 800-53 sono generalmente applicabili ai sistemi informativi federali degli Stati Uniti. Si tratta in genere di sistemi che devono essere sottoposti a un processo di valutazione e autorizzazione formale. Questo processo garantisce una protezione sufficiente della riservatezza, dell'integrità e della disponibilità delle informazioni e dei sistemi informativi. Tale protezione si basa sulla categoria di sicurezza e sul livello di impatto del sistema (basso, moderato o elevato), nonché sulla determinazione del rischio. I controlli di sicurezza sono selezionati dal catalogo di controlli di sicurezza NIST SP 800-53 e il sistema viene valutato rispetto a tali requisiti di controllo della sicurezza.

Il framework NIST SP 800-53 rappresenta i controlli di sicurezza e le procedure di valutazione associate definiti in NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations. Per eventuali discrepanze rilevate nel contenuto tra questo framework NIST SP 800-53 e l'ultima pubblicazione speciale NIST SP 800-53 Revisione 5, fai riferimento ai documenti ufficiali pubblicati disponibili presso il Centro risorse per la sicurezza informatica NIST.

Utilizzo di questo framework

È possibile utilizzare il framework NIST SP 800-53 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti NIST. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework NIST SP 800-53. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le

prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
NIST 800-53 Rev 5: Controlli di sicurezza e privacy per sistemi informativi e organizzazioni	634	373	20

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file AuditManager_ ConfigDataSourceMappings _NIST-800-53-Rev-5.zip.

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard NIST. Inoltre, non possono garantire che supererai un audit del NIST. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- National Institute of Standards and Technology (NIST)
- Centro risorse per la sicurezza informatica NIST
- AWS Pagina sulla conformità per il NIST

NIST Cybersecurity Framework v1.1

AWS Audit Manager fornisce un framework predefinito che supporta il NIST Cybersecurity Framework (CSF) v1.1.

> **Note**
>
> - Per informazioni sul framework Audit Manager che supporta NIST SP 800-53, vedere. NIST SP 800-53 Rev. 5
> - Per informazioni sul framework Audit Manager che supporta NIST SP 800-171, vedere. NIST SP 800-171 Rev. 2

Argomenti

Cos'è il framework NIST per la sicurezza informatica?

Il National Institute of Standards and Technology (NIST) è stato fondato nel 1901 e ora fa parte del Dipartimento del Commercio degli Stati Uniti. Il NIST è uno dei più antichi laboratori di scienze fisiche degli Stati Uniti. Il Congresso degli Stati Uniti istituì l'agenzia per migliorare quella che all'epoca era un'infrastruttura di misurazione di seconda categoria. L'infrastruttura rappresentava una sfida importante per la competitività industriale degli Stati Uniti, essendo rimasta indietro rispetto ad altre potenze economiche come il Regno Unito e la Germania.

Gli Stati Uniti dipendono dal funzionamento affidabile delle infrastrutture critiche. Le minacce alla sicurezza informatica sfruttano la maggiore complessità e interconnessione dei sistemi di infrastrutture critiche. Mettono a rischio la sicurezza, l'economia, la sicurezza e la salute pubblica degli Stati Uniti. Analogamente ai rischi finanziari e reputazionali, il rischio di sicurezza informatica influisce sui profitti di un'azienda. È in grado di far aumentare i costi e influire sui ricavi. Può danneggiare la capacità di un'organizzazione di innovare, conquistare e fidelizzare i clienti. In definitiva, la sicurezza informatica può amplificare la gestione complessiva del rischio di un'organizzazione.

Il framework NIST per la sicurezza informatica (CSF) è supportato da governi e industrie di tutto il mondo come base di riferimento consigliata per l'uso da parte di qualsiasi organizzazione, indipendentemente dal settore o dalle dimensioni. Il framework NIST per la sicurezza informatica è costituito da tre componenti principali: i principi fondamentali del framework, i profili e i livelli di implementazione. I principi fondamentali del framework contengono le attività e i risultati di sicurezza informatica desiderati organizzati in 23 categorie che coprono l'ampia gamma di obiettivi di sicurezza informatica per un'organizzazione. I profili contengono l'allineamento unico di un'organizzazione tra requisiti e obiettivi organizzativi, propensione al rischio e risorse, utilizzando i risultati desiderati del framework core. I livelli di implementazione descrivono il grado in cui le pratiche di gestione del rischio di sicurezza informatica di un'organizzazione presentano le caratteristiche definite nei principi fondamentali del framework.

Utilizzo di questo framework

È possibile utilizzare il NIST CSF v1.1 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti NIST CSF. Audit Manager attualmente supporta il componente principale del framework. Gestione audit non supporta il profilo e i componenti di implementazione in questo framework.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa in base ai controlli definiti nel NIST CSF. Quando è il momento di un audit, tu, o un delegato di tua scelta, potete esaminare le prove raccolte da Audit Manager. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
NIST Cybersecurity Framework (CSF) v1.1	49	59	22

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file AuditManager_ ConfigDataSourceMappings _NIST-CSF-v1.1.zip.

I controlli offerti da Audit Manager non hanno lo scopo di verificare se i sistemi sono conformi al NIST CSF. Inoltre, non possono garantire il superamento di un audit NIST. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- National Institute of Standards and Technology (NIST)
- Centro risorse per la sicurezza informatica NIST
- AWS Pagina sulla conformità per il NIST
- NIST Cybersecurity Framework: allineamento al NIST CSF nel cloud AWS

NIST SP 800-171 Rev. 2

AWS Audit Manager fornisce un framework standard predefinito che supporta NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

> **Note**
>
> - Per informazioni sul framework Audit Manager che supporta NIST SP 800-53, vedere. NIST SP 800-53 Rev. 5
> - Per informazioni sul framework Audit Manager che supporta NIST CSF, vedere. NIST Cybersecurity Framework v1.1

Argomenti

Che cos'è lo standard NIST SP 800-171?

NIST SP 800-171 si concentra sulla protezione della riservatezza delle informazioni controllate non classificate (CUI) in sistemi e organizzazioni non federali. Raccomanda requisiti di sicurezza specifici per raggiungere tale obiettivo. NIST 800-171 è una pubblicazione che delinea gli standard e le pratiche di sicurezza richiesti per le organizzazioni non federali che gestiscono il CUI sulle proprie reti. È stato pubblicato per la prima volta nel giugno 2015 dal National Institute of Standards and Technology (NIST). Il NIST è un'agenzia governativa degli Stati Uniti che ha pubblicato diversi standard e pubblicazioni per rafforzare la resilienza della sicurezza informatica nei settori pubblico e privato. NIST SP 800-171 ha ricevuto aggiornamenti regolari in linea con le minacce informatiche emergenti e le tecnologie in evoluzione. L'ultima versione (revisione 2) è stata rilasciata a febbraio 2020.

I controlli di sicurezza informatica all'interno del NIST SP 800-171 salvaguardano il CUI nelle reti IT di appaltatori e subappaltatori governativi. Definisce le pratiche e le procedure a cui gli appaltatori

governativi devono attenersi quando le loro reti elaborano o archiviano le CUI. Il NIST SP 800-171 si applica solo alle parti della rete di un appaltatore in cui è presente il CUI.

Utilizzo di questo framework

È possibile utilizzare il framework NIST SP 800-171 per prepararsi agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti NIST. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework NIST SP 800-171. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
NIST 800-171 Revisione 2: Protezione delle informazioni non classificate controllate in sistemi e organizzazioni non federali	81	29	14

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle origini dati in questo framework standard, scaricate il file _ _NIST-800-171-Rev-2.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi al NIST 800-171. Inoltre, non possono garantire il superamento di un audit NIST. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- National Institute of Standards and Technology (NIST)
- Centro risorse per la sicurezza informatica NIST
- AWS Pagina sulla conformità per il NIST

PCI DSS V3.2.1

AWS Audit Manager fornisce un framework standard predefinito che supporta il Payment Card Industry Data Security Standard (PCI DSS) v3.2.1.

> **Note**
>
> Per informazioni su PCI DSS v4 e sul framework di Gestione audit che lo supporta, consulta PCI DSS V4.0.

Argomenti

- Che cos'è PCI DSS?
- Utilizzo di questo framework a supporto della preparazione dell'audit

- Passaggi successivi
- Risorse aggiuntive

Che cos'è PCI DSS?

PCI DSS è uno standard proprietario per la sicurezza delle informazioni. È amministrato dal PCI Security Standards Council, fondato da American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. Il PCI DSS si applica alle entità che archiviano, elaborano o trasmettono dati dei titolari di carte (CHD) o dati di autenticazione sensibili (SAD). Tra le entità figurano, a titolo esemplificativo, commercianti, processori, acquirenti, emittenti e fornitori di servizi. Lo standard PCI DSS è imposto dai brand delle carte di credito ed è gestito dal Payment Card Industry Security Standards Council.

AWS è certificato come fornitore di servizi PCI DSS di livello 1, che rappresenta il livello di valutazione più elevato disponibile. La valutazione della conformità è stata condotta da Coalfire Systems Inc., un Qualified Security Assessor (QSA) indipendente. L'attestato di conformità PCI DSS (AOC) e il riepilogo delle responsabilità sono disponibili tramite. AWS Artifact Si tratta di un portale self-service per l'accesso su richiesta ai report di conformità. AWS Accedi alla console di AWS gestione o scopri di piùAWS Artifact nella sezione Guida introduttiva a. AWS Artifact

Puoi scaricare lo standard PCI DSS dalla libreria dei documenti PCI Security Standards Council.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework PCI DSS V3.2.1 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti PCI DSS. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa sulla base dei controlli definiti nel framework PCI DSS V3.2.1. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	168	116	15

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il file _ _PCI-DSS-v3.2.1.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard PCI DSS. Inoltre, non possono garantire che supererai un audit PCI DSS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- PCI Security Standards Council
- Libreria dei documenti del PCI Security Standards Council.
- AWS Pagina di conformità per PCI DSS

PCI DSS V4.0

AWS Audit Manager fornisce un framework predefinito che supporta il Payment Card Industry Data Security Standard (PCI DSS) v4.0.

> **Note**
>
> Per informazioni su PCI DSS v3.2.1 e sul framework di Gestione audit che lo supporta, consulta PCI DSS V3.2.1.

Argomenti

Che cos'è PCI DSS?

Il PCI DSS (Payment Card Industry Data Security Standard) è uno standard globale che fornisce una base di requisiti tecnici e operativi per la protezione dei dati di pagamento. PCI DSS v4.0 è la prossima evoluzione dello standard.

PCI DSS è stato sviluppato per incoraggiare e migliorare la sicurezza dei dati delle carte di pagamento. Inoltre, facilita l'ampia adozione di misure di sicurezza dei dati coerenti a livello globale. Fornisce una base di requisiti tecnici e operativi progettati per proteggere i dati delle carte di pagamento. Sebbene sia stato progettato specificamente per gli ambienti in cui sono presenti i dati delle carte di pagamento, è possibile utilizzare gli standard PCI DSS per proteggersi dalle minacce e proteggere altri elementi dell'ecosistema dei pagamenti.

Il PCI Security Standards Council (PCI SSC) ha introdotto molte modifiche tra PCI DSS v3.2.1 e v4.0. Questi aggiornamenti sono suddivisi in tre categorie:

1. Requisiti in evoluzione: modifiche per garantire che lo standard sia aggiornato alle minacce e alle tecnologie emergenti e ai cambiamenti nel settore dei pagamenti. Alcuni esempi sono i requisiti o le procedure di test nuovi o modificati oppure l'eliminazione di un requisito.

2. Chiarimenti o indicazioni: aggiornamenti a formulazioni, spiegazioni, definizioni, indicazioni aggiuntive o istruzioni per aumentare la comprensione o fornire ulteriori informazioni o indicazioni su un particolare argomento.
3. Struttura o formato: riorganizzazione dei contenuti, compresa la combinazione, la separazione e la rinumerazione dei requisiti per allineare i contenuti.

Utilizzo di questo framework a supporto della preparazione dell'audit

> **Note**
>
> Questo framework standard utilizza i controlli consolidati della Centrale di sicurezza come origine dati. Per raccogliere correttamente le prove dai controlli consolidati, assicurati di aver attivato l'impostazione dei risultati del controllo consolidato in Centrale di sicurezza. Per ulteriori informazioni sull'utilizzo della Centrale di sicurezza come tipo di origine dati, consulta Controlli AWS Security Hub supportati da AWS Audit Manager.

Puoi utilizzare il framework PCI DSS V4.0 per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controlli in base ai requisiti PCI DSS V4.0. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. Lo fa in base ai controlli definiti nel framework PCI DSS V4.0. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Standard di sicurezza dei dati del settore delle carte di pagamento (PCI DSS) v4.0	175	105	15

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il file _ _PCI-DSS-v4.0.zip. AuditManager ConfigDataSourceMappings

I controlli di questo AWS Audit Manager framework non hanno lo scopo di verificare se i sistemi sono conformi allo standard PCI DSS. Inoltre, non possono garantire che supererai un audit PCI DSS. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- Hub di risorse PCI DSS v4.0
- PCI Security Standards Council
- Libreria dei documenti del PCI Security Standards Council.
- AWS Pagina di conformità per PCI DSS

- Guida alla conformità relativa allo standard PCI DSS (Payment Card Industry Data Security Standard) v4.0 AWS

SSAE-18 SOC 2

AWS Audit Manager fornisce un framework standard predefinito che supporta lo Statement on Standards for Attestations Engagement (SSAE) n. 18, Service Organizations Controls (SOC) Report 2.

Argomenti

- Che cos'è SOC 2?
- Utilizzo di questo framework a supporto della preparazione dell'audit
- Passaggi successivi
- Risorse aggiuntive

Che cos'è SOC 2?

SOC 2, definito dall'American Institute of Certified Public Accountants (AICPA), è il nome di una serie di report prodotti durante un audit. È destinato alle organizzazioni di servizi (organizzazioni che forniscono sistemi informativi come servizio ad altre organizzazioni) per emettere report convalidati sui controlli interni su tali sistemi informativi agli utenti di tali servizi. I report si concentrano sui controlli raggruppati in cinque categorie note come Trust Service Principles.

AWS I report SOC sono rapporti di esame indipendenti di terze parti che dimostrano come AWS raggiungere i controlli e gli obiettivi chiave di conformità. Lo scopo di questi report è aiutare voi e i vostri revisori a comprendere i AWS controlli stabiliti per supportare le operazioni e la conformità. Esistono cinque rapporti AWS SOC:

- AWS Rapporto SOC 1, disponibile per AWS i clienti da. AWS Artifact
- AWS Rapporto SOC 2 su sicurezza, disponibilità e riservatezza, disponibile per AWS i clienti da. AWS Artifact
- AWS Report SOC 2 su sicurezza, disponibilità e riservatezza disponibile per AWS i clienti da AWS Artifact(l'ambito include solo Amazon DocumentDB).
- AWS Report SOC 2 sulla privacy di tipo I, disponibile per i clienti da AWS . AWS Artifact

- AWS Report SOC 3 su sicurezza, disponibilità e riservatezza, disponibile al pubblico come white paper.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare questo framework per prepararti agli audit. Questo framework include una raccolta predefinita di controlli con descrizioni e procedure di test. Questi controlli sono raggruppati in set di controllo in base ai requisiti SOC 2. Puoi inoltre personalizzare questo framework e i relativi controlli per supportare gli audit interni in base ai requisiti specifici.

Utilizzando il framework come punto di partenza, puoi creare una valutazione Gestione audit e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue AWS risorse. La valutazione avviene sulla base dei controlli definiti nel framework. Quando è il momento di fare un audit, tu o un delegato di tua scelta potete esaminare le prove raccolte da Gestione audit. A seconda dei casi, puoi sfogliare le cartelle delle prove della valutazione e scegliere quali prove includere nel report di valutazione. Oppure, se hai abilitato la ricerca delle prove, puoi cercare prove specifiche ed esportarle in formato CSV oppure creare un report di valutazione dai risultati della ricerca. In ogni caso, puoi utilizzare questo report di valutazione per dimostrare che i controlli funzionano come previsto.

I dettagli del framework sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo
Dichiarazione sugli Standard for Attestations Engagement (SSAE) n. 18, Service Organizations Controls (SOC) Report 2	46	15	20

> **Tip**
>
> Per esaminare le AWS Config regole utilizzate come mappature delle sorgenti dati in questo framework standard, scaricate il file _ _SSAE-no.-18-soc-report-2.zip. AuditManager ConfigDataSourceMappings

I controlli di questo framework non hanno lo scopo di verificare se i sistemi sono conformi. AWS Audit Manager Inoltre, non possono garantire che supererai un audit. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

È possibile trovare questo framework nella scheda Standard frameworks della libreria di framework in Audit Manager.

Passaggi successivi

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta. Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Risorse aggiuntive

- AWS Pagina di conformità per SOC

Tipi di fonti di dati supportati per prove automatizzate

Quando crei un controllo personalizzato in AWS Audit Manager, puoi impostare il controllo per raccogliere prove automatiche dai seguenti tipi di fonti di dati:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Chiamate API

Ogni tipo di fonte di dati offre funzionalità distinte per l'acquisizione dei registri delle attività degli utenti, dei risultati di conformità, delle configurazioni delle risorse e altro ancora.

In questo capitolo puoi conoscere ciascuno di questi tipi di origini dati automatizzate e i AWS Security Hub controlli, AWS Config le regole e le chiamate AWS API specifici supportati da Audit Manager.

Punti chiave

La tabella seguente fornisce una panoramica di ogni tipo automatizzato di origine dati.

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Per utilizzare questo tipo di fonte dati...	Quando questo controllo è attivo in una valutazione...	Suggerimenti correlati per la risoluzione dei problemi
AWS CloudTrail	Tiene traccia di un'attività specifica dell'utente.	Continuo.	Seleziona dall'elenco dei nomi di eventi supportati.	Audit Manager filtra CloudTrail i log in base alla parola chiave scelta. I risultati vengono	La mia valutazione non sta

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Per utilizzare questo tipo di fonte dati...	Quando questo controllo è attivo in una valutazione...	Suggerimenti correlati per la risoluzione dei problemi
				importati come prove dell'attività dell'utente.	raccogliendo prove dell'attività degli utenti da AWS CloudTrail

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Per utilizzare questo tipo di fonte dati...	Quando questo controllo è attivo in una valutazione...	Suggerimenti correlati per la risoluzione dei problemi
AWS Config	Acquisisce un'istantanea del vostro stato di sicurezza delle risorse riportando i risultati di. AWS Config	In base ai trigger definiti nella regola. AWS Config	Scegli una regola, quindi seleziona una regola. • Per le regole gestite, seleziona dall'elenco delle parole chiave supportate per le regole gestite. • Per le regole personalizzate, seleziona dall'elenco delle regole disponibili.	Audit Manager ottiene i risultati di questa regola direttamente da AWS Config. Il risultato viene importato come prova del controllo di conformità.	La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Config AWS Config problemi di integrazione

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Per utilizzare questo tipo di fonte dati...	Quando questo controllo è attivo in una valutazione...	Suggerimenti correlati per la risoluzione dei problemi
AWS Security Hub	Acquisisce uno snapshot della posizione di sicurezza delle risorse segnalando gli esiti da Security Hub.	In base alla pianificazione del controllo Security Hub.	Seleziona dall'elenco degli ID di controllo Security Hub supportati.	Gestione audit ottiene il risultato del controllo di sicurezza direttamente Security Hub. Il risultato viene importato come prova del controllo di conformità.	La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Per utilizzare questo tipo di fonte dati...	Quando questo controllo è attivo in una valutazione...	Suggerimenti correlati per la risoluzione dei problemi
AWS chiamata API	Scatta un'istantanea della configurazione delle risorse direttamente tramite una chiamata API all'indirizzo specificato Servizio AWS.	Giornaliero, settimanale o mensile.	Seleziona dall'elenco delle chiamate API supportate, quindi seleziona la frequenza preferita.	Gestione audit effettua la chiamata API in base alla frequenza specificata. La risposta viene importata come prova dei dati di configurazione.	La mia valutazione non sta raccogliendo prove dei dati di configurazione per una chiamata AWS API

> **Tip**
>
> È possibile creare controlli personalizzati che raccolgono prove utilizzando raggruppamenti predefiniti delle fonti di dati di cui sopra. Questi raggruppamenti di fonti di dati sono noti come AWS fonti gestite. Ogni fonte AWS gestita rappresenta un controllo comune o un controllo di base che si allinea a un requisito di conformità comune. Questo ti offre un modo efficiente per

mappare i requisiti di conformità a un gruppo pertinente di fonti di AWS dati. Per visualizzare i controlli comuni disponibili, consultaIndividuazione dei controlli disponibili in AWS Audit Manager.
In alternativa, puoi utilizzare i quattro tipi di fonti di dati precedenti per definire fonti di dati personalizzate. Ciò offre la flessibilità necessaria per caricare prove manuali o raccogliere prove automatizzate da una risorsa specifica dell'azienda, ad esempio una regola personalizzata AWS Config .

Passaggi successivi

Per ulteriori informazioni sulle fonti di dati specifiche che puoi utilizzare nei controlli personalizzati, consulta le pagine seguenti.

- Regole di AWS Config supportato da AWS Audit Manager
- AWS Security Hub controlli supportati da AWS Audit Manager
- AWS Chiamate API supportate da AWS Audit Manager
- AWS CloudTrail nomi di eventi supportati da AWS Audit Manager

Regole di AWS Config supportato da AWS Audit Manager

È possibile utilizzare Audit Manager per acquisire le AWS Config valutazioni come prove per gli audit. Quando si crea o si modifica un controllo personalizzato, è possibile specificare una o più AWS Config regole come mappatura della fonte di dati per la raccolta delle prove. AWS Config esegue controlli di conformità in base a queste regole e Audit Manager riporta i risultati come prova del controllo di conformità.

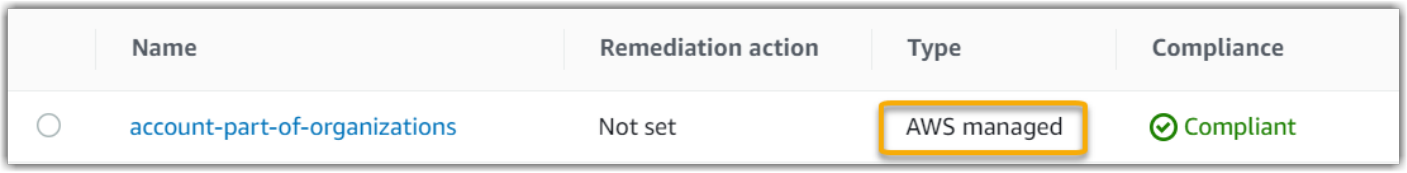
Oltre alle regole gestite, puoi anche mappare le regole personalizzate a una fonte di dati di controllo.

Indice

Punti chiave

- Gestione audit non raccoglie prove dalle regole AWS Config collegate ai servizi, ad eccezione delle regole collegate ai servizi dei Pacchetti di conformità e di AWS Organizations.
- Audit Manager non gestisce AWS Config le regole per te. Prima di iniziare la raccolta delle prove, ti consigliamo di rivedere i parametri delle AWS Config regole correnti. Quindi, convalida tali parametri in base ai requisiti del framework prescelto. Se necessario, puoi aggiornare i parametri di una regola in AWS Configaffinché sia allineata ai requisiti del framework. Ciò contribuirà a garantire che le valutazioni raccolgano le prove di verifica della conformità corrette per quel framework.

  Ad esempio, supponiamo che tu stia creando una valutazione per CIS v1.2.0. Questo framework ha un controllo denominato Ensure IAM Password Policy che richiede una lunghezza minima di 14 o più. In AWS Config, la iam-password-policyregola ha un `MinimumPasswordLength` parametro che controlla la lunghezza della password. Il valore predefinito per questo parametro è 14 caratteri. Di conseguenza, la regola è conforme ai requisiti di controllo. Se non utilizzi il valore del parametro predefinito, assicurati che il valore che stai utilizzando sia uguale o superiore ai 14 caratteri richiesti dal CIS v1.2.0. Puoi trovare i dettagli dei parametri predefiniti per ogni regola gestita nella documentazione AWS Config.
- Se devi verificare se una AWS Config regola è una regola gestita o una regola personalizzata, puoi farlo utilizzando la AWS Config console. Dal menu di navigazione a sinistra, scegli Regole e cerca la regola nella tabella. Se si tratta di una regola gestita, la colonna Tipo mostra AWS gestita.



Regole AWS Config gestite supportate

Le seguenti regole AWS Config gestite sono supportate da Audit Manager. Puoi utilizzare una delle seguenti parole chiave di identificazione delle regole gestite quando configuri un'origine dati per un controllo personalizzato. Per ulteriori informazioni sulle regole gestite elencate di seguito, scegli un elemento dall'elenco o consulta AWS Config Regole gestite nella Guida per l'utente AWS Config .

> **Tip**
>
> Quando scegli una regola gestita nella console Gestione audit durante la creazione di controlli personalizzati, assicurati di cercare una delle seguenti parole chiave identificative

delle regole e non il nome della regola. Per informazioni sulla differenza tra il nome della regola e l'identificatore della regola e su come trovare l'identificatore per una regola gestita, consulta la sezione Risoluzione dei problemi di questa guida per l'utente.

Parole chiave AWS Config gestite supportate

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Parole chiave AWS Config gestite supportate

- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Parole chiave AWS Config gestite supportate

- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY

Parole chiave AWS Config gestite supportate

- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Parole chiave AWS Config gestite supportate

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _ABILITATO AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- UTENTE ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN

Parole chiave AWS Config gestite supportate

- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Parole chiave AWS Config gestite supportate

- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED

Parole chiave AWS Config gestite supportate

- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- PACCHETTI NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST

Parole chiave AWS Config gestite supportate

- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED

Parole chiave AWS Config gestite supportate

- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK

Parole chiave AWS Config gestite supportate

- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- MACCHINA VIRTUALE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK

Parole chiave AWS Config gestite supportate

- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Utilizzo di regole AWS Config personalizzate con Audit Manager

È possibile utilizzare regole AWS Config personalizzate come fonte di dati per la creazione di report di audit. Quando un controllo ha un'origine dati mappata su una AWS Config regola, Audit Manager aggiunge la valutazione creata dalla AWS Config regola.

Le regole personalizzate che è possibile utilizzare dipendono dal dispositivo con Account AWS cui si accede all'Audit Manager. Se è possibile accedere a una regola personalizzata in AWS Config, è possibile utilizzarla come mappatura dell'origine dati in Audit Manager.

- Per uso individuale Account AWS: puoi utilizzare qualsiasi regola personalizzata creata con il tuo account.
- Per gli account che fanno parte di un'organizzazione: in entrambi i casi, puoi utilizzare qualsiasi regola personalizzata a livello di membro. In alternativa, puoi utilizzare una qualsiasi delle regole personalizzate a livello di organizzazione disponibili in AWS Config.

Dopo aver mappato le regole personalizzate come origine dati per un controllo, puoi aggiungere quel controllo a un framework personalizzato in Audit Manager.

Risorse aggiuntive

- Per trovare assistenza sui problemi relativi a questo tipo di origine dati, consulta La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Config e problemi di AWS Config integrazione.
- Per creare un controllo personalizzato utilizzando questo tipo di origine dati, consultaCreazione di un controllo personalizzato in AWS Audit Manager.
- Per creare un framework personalizzato che utilizzi il tuo controllo personalizzato, consultaCreazione di un framework personalizzato in AWS Audit Manager.
- Per aggiungere il controllo personalizzato a un framework personalizzato esistente, vedereModifica di un framework personalizzato in AWS Audit Manager.
- Per creare una regola personalizzata in AWS Config, consulta Sviluppo di una regola personalizzata AWS Config nella Guida per gli AWS Config sviluppatori.

AWS Security Hub controlli supportati da AWS Audit Manager

È possibile utilizzare Audit Manager per acquisire i risultati del Security Hub come prova per gli audit. Quando si crea o si modifica un controllo personalizzato, è possibile specificare uno o più controlli Security Hub come mappatura dell'origine dati per la raccolta di prove. Security Hub esegue controlli di conformità basati su questi controlli e Audit Manager riporta i risultati come prova del controllo di conformità.

Indice

Punti chiave

- Audit Manager non raccoglie prove dalle AWS Config regole collegate ai servizi create da Security Hub.
- Il 9 novembre 2022, Security Hub ha lanciato controlli di sicurezza automatizzati allineati ai requisiti Foundations Benchmark versione 1.4.0 del Center for Internet Security (CIS) AWS Foundations

Benchmark, Level 1 e 2 (CIS v1.4.0). In Security Hub, lo standard CIS v1.4.0 è supportato in aggiunta allo standard CIS v1.2.0.

- Ti consigliamo di attivare l'impostazione dei risultati del controllo consolidato nel Security Hub se non è già attivata. Se si attiva Security Hub a partire dal 23 febbraio 2003, questa impostazione è attivata per impostazione predefinita.

  Quando i risultati consolidati sono abilitati, Security Hub produce un singolo risultato per ogni controllo di sicurezza (anche quando lo stesso controllo si applica a più standard). Ogni risultato Security Hub viene raccolto come un'unica valutazione delle risorse in Gestione audit. Di conseguenza, i risultati consolidati comportano una diminuzione delle valutazioni totali delle risorse uniche eseguite da Gestione audit per i risultati Security Hub. Per tale motivo, l'utilizzo di risultati consolidati può spesso portare a una riduzione dei costi di utilizzo di Gestione audit, senza sacrificare la qualità e la disponibilità delle prove. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Audit Manager.

Esempi di prove quando i risultati consolidati sono attivati o disattivati

Gli esempi seguenti mostrano un confronto tra il modo in cui Gestione audit raccoglie e presenta le prove a seconda delle impostazioni Security Hub.

When consolidated findings is turned on

Supponiamo che tu abbia abilitato i seguenti tre standard di sicurezza in Security Hub: AWS FSBP, PCI DSS e CIS Benchmark v1.2.0.

- Tutti e tre questi standard utilizzano lo stesso controllo (IAM.4) con la stessa regola di base (-check). AWS Config iam-root-access-key
- Poiché l'impostazione dei risultati consolidati è attivata, Security Hub genera un singolo risultato per questo controllo.
- Security Hub invia i risultati consolidati a Gestione audit per questo controllo.
- Il risultato consolidato conta come un'unica valutazione delle risorse in Gestione audit. Di conseguenza, alla valutazione viene aggiunta una singola prova.

Di seguito è riportato un esempio di come potrebbero apparire le prove:

```
{
    "SchemaVersion": "2018-10-08",
```

```
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
```

```
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```


When consolidated findings is turned off

Supponiamo che tu abbia abilitato i seguenti tre standard di sicurezza in Security Hub: AWS FSBP, PCI DSS e CIS Benchmark v1.2.0.

- Tutti e tre questi standard utilizzano lo stesso controllo (IAM.4) con la stessa regola di base (-check). AWS Config iam-root-access-key

- Poiché l'impostazione degli esiti consolidati è disattivata, Security Hub genera un esito separato per controllo di sicurezza per ogni standard abilitato (in questo caso, tre esiti).
- Security Hub invia tre risultati separati specifici dello standard a Gestione audit per questo controllo.
- Il conteggio dei tre risultati come un'unica valutazione delle tre risorse in Gestione audit. Di conseguenza, vengono aggiunti tre elementi di prova distinti alla valutazione.

Di seguito è riportato un esempio di come potrebbero apparire le prove. Nota che in questo esempio, ciascuno dei tre payload seguenti ha lo stesso ID di controllo di sicurezza (*SecurityControlId":"IAM.4"*). Per questo motivo, il controllo di valutazione che raccoglie queste prove in Gestione audit (IAM.4) riceve tre prove separate quando i seguenti risultati arrivano da Security Hub.

Prove per IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
```

```
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.848Z",
            "LastObservedAt":"2023-11-01T14:12:04.106Z",
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
```

```
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
         }
      ]
   }
}
```

Prove per IAM.4 (CIS 1.2)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
```

```
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
```

```
                  "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:13.436Z"
      }
   ]
  }
}
```

Prove per PCI.IAM.1 (PCI DSS)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
```

```
            "SchemaVersion":"2018-10-08",
            "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
            "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "ProductName":"Security Hub",
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
```

```
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "RelatedRequirements":[
                 "PCI DSS 2.1",
                 "PCI DSS 2.2",
                 "PCI DSS 7.2.1"
              ],
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"standards/pci-dss/v/3.2.1"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
```

```
            ]
          },
          "ProcessedAt":"2023-11-01T14:12:05.950Z"
        }
      ]
    }
}
```

Controlli Security Hub supportati

I seguenti controlli Security Hub sono attualmente supportati da Gestione audit. Puoi utilizzare una delle seguenti parole chiave ID di controllo specifiche dello standard quando configuri un'origine dati per un controllo personalizzato.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
CIS versione 1.2.0	1.2	IAM.5
CIS versione 1.2.0	1.3	IAM.8
CIS versione 1.2.0	1.4	IAM.3
CIS versione 1.2.0	1.5	IAM.11
CIS versione 1.2.0	1.6	IAM.12
CIS versione 1.2.0	1,7	IAM.13
CIS versione 1.2.0	1.8	IAM.14
CIS versione 1.2.0	1.9	IAM.15
CIS versione 1.2.0	1.10	IAM.16

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
CIS versione 1.2.0	1.11	IAM.17
CIS versione 1.2.0	1.12	IAM.4
CIS versione 1.2.0	1.13	IAM.9
CIS versione 1.2.0	1.14	IAM.6
CIS versione 1.2.0	1.16	IAM.2
CIS versione 1.2.0	1.20	IAM.18
CIS versione 1.2.0	1,22	IAM.1
CIS versione 1.2.0	2.1	CloudTrail1.
CIS versione 1.2.0	2.2	CloudTrail4.
CIS versione 1.2.0	2.3	CloudTrail6.
CIS versione 1.2.0	2.4	CloudTrail5.
CIS versione 1.2.0	2.5	Config.1
CIS versione 1.2.0	2.6	CloudTrail7.
CIS versione 1.2.0	2.7	CloudTrail2.
CIS versione 1.2.0	2.8	KMS.4
CIS versione 1.2.0	2.9	EC2.6
CIS versione 1.2.0	3.1	CloudWatch2.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
CIS versione 1.2.0	3.2	CloudWatch3.
CIS versione 1.2.0	3.3	CloudWatch1.
CIS versione 1.2.0	3.4	CloudWatch4.
CIS versione 1.2.0	3.5	CloudWatch5.
CIS versione 1.2.0	3.6	CloudWatch6.
CIS versione 1.2.0	3.7	CloudWatch.7
CIS versione 1.2.0	3.8	CloudWatch8.
CIS versione 1.2.0	3.9	CloudWatch9.
CIS versione 1.2.0	3,10	CloudWatch.10
CIS versione 1.2.0	3,11	CloudWatch.11
CIS versione 1.2.0	3,12	CloudWatch.12
CIS versione 1.2.0	3.13	CloudWatch.13
CIS versione 1.2.0	3,14	CloudWatch.14
CIS versione 1.2.0	4.1	EC2.13
CIS versione 1.2.0	4.2	EC 2.14
CIS versione 1.2.0	4.3	EC 2.2

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
PCI DSS	FOTO. AutoScaling1.	AutoScaling.1.
PCI DSS	PCI. CloudTrail1.	CloudTrail.1.
PCI DSS	PCI. CloudTrail2.	CloudTrail2.
PCI DSS	PCI. CloudTrail3.	CloudTrail3.
PCI DSS	PCI. CloudTrail4.	CloudTrail4.
PCI DSS	PCI. CodeBuild 1.	CodeBuild.1.
PCI DSS	PCI. CodeBuild 2.	CodeBuild2.
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1.
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty 1.	GuardDuty.1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI. SageMaker 1.	SageMaker.1.
PCI DSS	PCI.SSM.1	SSM.1

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Migliori pratiche di sicurezza di base	Account.1	Account.1
AWS Le migliori pratiche di sicurezza di base	Account.2	Conto.2
AWS Migliori pratiche di sicurezza di base	ACM.1	ACM.1
AWS Le migliori pratiche di sicurezza di base	ACM.2	ACM.2
AWS Le migliori pratiche di sicurezza di base	APIGateway.1	APIGateway.1
AWS Le migliori pratiche di sicurezza di base	APIGateway.2	APIGateway.2
AWS Le migliori pratiche di sicurezza di base	APIGateway.3	APIGateway.3
AWS Le migliori pratiche di sicurezza di base	APIGateway.4	APIGateway.4
AWS Le migliori pratiche di sicurezza di base	APIGateway.5	APIGateway.5

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	APIGateway.8	APIGateway.8
AWS Le migliori pratiche di sicurezza di base	APIGateway.9	APIGateway.9
AWS Le migliori pratiche di sicurezza di base	AppSync2.	AppSync2.
AWS Migliori pratiche di sicurezza di base	AppSync5.	AppSync5.
AWS Migliori pratiche di sicurezza di base	Atena.1	Atena.1
AWS Le migliori pratiche di sicurezza di base	AutoScaling1.	AutoScaling.1.
AWS Migliori pratiche di sicurezza di base	AutoScaling2.	AutoScaling2.
AWS Migliori pratiche di sicurezza di base	AutoScaling3.	AutoScaling3.
AWS Migliori pratiche di sicurezza di base	AutoScaling4.	AutoScaling4.
AWS Migliori pratiche di sicurezza di base	Autoscaling.5	Autoscaling.5

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	AutoScaling6.	AutoScaling6.
AWS Migliori pratiche di sicurezza di base	AutoScaling9.	AutoScaling9.
AWS Migliori pratiche di sicurezza di base	Backup.1	Backup.1
AWS Le migliori pratiche di sicurezza di base	CloudForm ation1.	CloudFormation.1.
AWS Migliori pratiche di sicurezza di base	CloudFront1.	CloudFront.1.
AWS Migliori pratiche di sicurezza di base	CloudFront2.	CloudFront2.
AWS Migliori pratiche di sicurezza di base	CloudFront3.	CloudFront3.
AWS Migliori pratiche di sicurezza di base	CloudFront4.	CloudFront4.
AWS Migliori pratiche di sicurezza di base	CloudFront5.	CloudFront5.
AWS Migliori pratiche di sicurezza di base	CloudFront6.	CloudFront6.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	CloudFront7.	CloudFront7.
AWS Migliori pratiche di sicurezza di base	CloudFront8.	CloudFront8.
AWS Migliori pratiche di sicurezza di base	CloudFront9.	CloudFront9.
AWS Migliori pratiche di sicurezza di base	CloudFront.10	CloudFront.10
AWS Migliori pratiche di sicurezza di base	CloudFront1.2	CloudFront.12
AWS Migliori pratiche di sicurezza di base	CloudFront1.3	CloudFront.13
AWS Migliori pratiche di sicurezza di base	CloudTrail1.	CloudTrail.1.
AWS Migliori pratiche di sicurezza di base	CloudTrail2.	CloudTrail2.
AWS Migliori pratiche di sicurezza di base	CloudTrail3.	CloudTrail3.
AWS Migliori pratiche di sicurezza di base	CloudTrail4.	CloudTrail4.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	CloudTrail5.	CloudTrail5.
AWS Migliori pratiche di sicurezza di base	CloudTrail6.	CloudTrail6.
AWS Migliori pratiche di sicurezza di base	CloudTrail7.	CloudTrail7.
AWS Migliori pratiche di sicurezza di base	CloudWatch1.	CloudWatch.1.
AWS Migliori pratiche di sicurezza di base	CloudWatch2.	CloudWatch2.
AWS Migliori pratiche di sicurezza di base	CloudWatch3.	CloudWatch3.
AWS Migliori pratiche di sicurezza di base	CloudWatch4.	CloudWatch4.
AWS Migliori pratiche di sicurezza di base	CloudWatch5.	CloudWatch5.
AWS Migliori pratiche di sicurezza di base	CloudWatch6.	CloudWatch6.
AWS Migliori pratiche di sicurezza di base	CloudWatch7.	CloudWatch7.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	CloudWatch8.	CloudWatch8.
AWS Migliori pratiche di sicurezza di base	CloudWatch9.	CloudWatch9.
AWS Migliori pratiche di sicurezza di base	CloudWatch.10	CloudWatch.10
AWS Migliori pratiche di sicurezza di base	CloudWatch1.1	CloudWatch.11
AWS Migliori pratiche di sicurezza di base	CloudWatch1.2	CloudWatch.12
AWS Migliori pratiche di sicurezza di base	CloudWatch1.3	CloudWatch.13
AWS Migliori pratiche di sicurezza di base	CloudWatch1.4	CloudWatch.14
AWS Migliori pratiche di sicurezza di base	CloudWatch1.5	CloudWatch.15
AWS Migliori pratiche di sicurezza di base	CloudWatch1.6	CloudWatch.16
AWS Migliori pratiche di sicurezza di base	CloudWatch1.7	CloudWatch.17

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	CodeBuild1.	CodeBuild.1.
AWS Migliori pratiche di sicurezza di base	CodeBuild2.	CodeBuild2.
AWS Migliori pratiche di sicurezza di base	CodeBuild3.	CodeBuild3.
AWS Migliori pratiche di sicurezza di base	CodeBuild4.	CodeBuild4.
AWS Migliori pratiche di sicurezza di base	CodeBuild5.	CodeBuild5.
AWS Migliori pratiche di sicurezza di base	Config.1	Config.1
AWS Le migliori pratiche di sicurezza di base	DMS.1	DMS.1
AWS Le migliori pratiche di sicurezza di base	DMS.6	DMS.6
AWS Migliori pratiche di sicurezza di base	DMS.7	DMS.7
AWS Le migliori pratiche di sicurezza di base	DMS.8	DMS.8

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	DMS.9	DMS.9
AWS Le migliori pratiche di sicurezza di base	Documento DB.1	Documento DB.1
AWS Le migliori pratiche di sicurezza di base	Documento DB.2	Documento DB.2
AWS Le migliori pratiche di sicurezza di base	Documento DB.3	Documento DB.3
AWS Le migliori pratiche di sicurezza di base	Documento DB.4	Documento DB.4
AWS Le migliori pratiche di sicurezza di base	Documento DB.5	Documento DB.5
AWS Le migliori pratiche di sicurezza di base	DynamoDB.1	DynamoDB.1
AWS Le migliori pratiche di sicurezza di base	DynamoDB.2	DynamoDB.2
AWS Le migliori pratiche di sicurezza di base	DynamoDB.3	DynamoDB.3
AWS Le migliori pratiche di sicurezza di base	Dynamo DB.4	Dynamo DB.4

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	Dynamo DB.6	Dynamo DB.6
AWS Le migliori pratiche di sicurezza di base	EC2.1	EC2.1
AWS Le migliori pratiche di sicurezza di base	EC2.2	EC2.2
AWS Le migliori pratiche di sicurezza di base	EC2.3	EC2.3
AWS Le migliori pratiche di sicurezza di base	EC2.4	EC2.4
AWS Le migliori pratiche di sicurezza di base	EC2.6	EC2.6
AWS Le migliori pratiche di sicurezza di base	EC2.7	EC2.7
AWS Le migliori pratiche di sicurezza di base	EC2.8	EC2.8
AWS Le migliori pratiche di sicurezza di base	EC2.9	EC2.9
AWS Le migliori pratiche di sicurezza di base	EC2.10	EC2.10

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	EC2.12	EC2.12
AWS Le migliori pratiche di sicurezza di base	EC2.13	EC2.13
AWS Le migliori pratiche di sicurezza di base	EC 2.14	EC 2.14
AWS Le migliori pratiche di sicurezza di base	EC2.15	EC2.15
AWS Le migliori pratiche di sicurezza di base	EC2.16	EC2.16
AWS Le migliori pratiche di sicurezza di base	EC2.17	EC2.17
AWS Le migliori pratiche di sicurezza di base	EC2.18	EC2.18
AWS Le migliori pratiche di sicurezza di base	EC2.19	EC2.19
AWS Le migliori pratiche di sicurezza di base	EC2.20	EC2.20
AWS Le migliori pratiche di sicurezza di base	EC2.21	EC2.21

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	EC2.22	EC2.22
AWS Le migliori pratiche di sicurezza di base	EC2.23	EC2.23
AWS Le migliori pratiche di sicurezza di base	EC2.24	EC2.24
AWS Le migliori pratiche di sicurezza di base	EC2.25	EC2.25
AWS Le migliori pratiche di sicurezza di base	EC2.28	EC2,28
AWS Migliori pratiche di sicurezza di base	EC2.51	EC2,51
AWS Migliori pratiche di sicurezza di base	ECR.1	ECR.1
AWS Le migliori pratiche di sicurezza di base	ECR.2	ECR.2
AWS Le migliori pratiche di sicurezza di base	ECR.3	ECR.3
AWS Le migliori pratiche di sicurezza di base	ECS.1	ECS.1

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	ECS.2	ECS.2
AWS Le migliori pratiche di sicurezza di base	ECS.3	ECS.3
AWS Le migliori pratiche di sicurezza di base	ECS.4	ECS.4
AWS Le migliori pratiche di sicurezza di base	ECS.5	ECS.5
AWS Le migliori pratiche di sicurezza di base	ECS.8	ECS.8
AWS Le migliori pratiche di sicurezza di base	ECS.9	ECS.9
AWS Migliori pratiche di sicurezza di base	ECS.10	ECS.10
AWS Le migliori pratiche di sicurezza di base	ECS.12	ECS.12
AWS Le migliori pratiche di sicurezza di base	EFS.1	EFS.1
AWS Le migliori pratiche di sicurezza di base	EFS.2	EFS.2

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	EFS.3	EFS.3
AWS Le migliori pratiche di sicurezza di base	EFS.4	EFS.4
AWS Le migliori pratiche di sicurezza di base	EKS.1	EKS.1
AWS Le migliori pratiche di sicurezza di base	EKS.2	EKS.2
AWS Le migliori pratiche di sicurezza di base	EKS.8	EKS.8
AWS Migliori pratiche di sicurezza di base	ElastiCache1.	ElastiCache.1.
AWS Migliori pratiche di sicurezza di base	ElastiCache2.	ElastiCache2.
AWS Migliori pratiche di sicurezza di base	ElastiCache3.	ElastiCache3.
AWS Migliori pratiche di sicurezza di base	ElastiCache4.	ElastiCache4.
AWS Migliori pratiche di sicurezza di base	ElastiCache5.	ElastiCache5.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	ElastiCache6.	ElastiCache6.
AWS Migliori pratiche di sicurezza di base	ElastiCache7.	ElastiCache7.
AWS Migliori pratiche di sicurezza di base	ElasticBeanstalk1.	ElasticBeanstalk.1.
AWS Migliori pratiche di sicurezza di base	ElasticBeanstalk2.	ElasticBeanstalk2.
AWS Migliori pratiche di sicurezza di base	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Migliori pratiche di sicurezza di base	ELB.1	ELB.1
AWS Le migliori pratiche di sicurezza di base	ELB.2	ELB.2
AWS Le migliori pratiche di sicurezza di base	ELB.3	ELB.3
AWS Le migliori pratiche di sicurezza di base	ELB.4	ELB.4
AWS Le migliori pratiche di sicurezza di base	ELB.5	ELB.5

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	ELB.6	ELB.6
AWS Migliori pratiche di sicurezza di base	ELB.7	ELB.7
AWS Migliori pratiche di sicurezza di base	ELB.8	ELB.8
AWS Migliori pratiche di sicurezza di base	ELB.9	ELB.9
AWS Migliori pratiche di sicurezza di base	ELB.10	ELB.10
AWS Migliori pratiche di sicurezza di base	ELB.12	ELB.12
AWS Migliori pratiche di sicurezza di base	ELB.13	ELB.13
AWS Migliori pratiche di sicurezza di base	ELB.14	ELB.14
AWS Migliori pratiche di sicurezza di base	PAGINA 16	ELB.16
AWS Migliori pratiche di sicurezza di base	ELBv2.1	ELB.1

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	EMR.1	EMR.1
AWS Migliori pratiche di sicurezza di base	EMR.2	EMR.2
AWS Migliori pratiche di sicurezza di base	ES.1	ES.1
AWS Migliori pratiche di sicurezza di base	ES.2	ES.2
AWS Migliori pratiche di sicurezza di base	ES.3	ES.3
AWS Migliori pratiche di sicurezza di base	ES.4	ES.4
AWS Migliori pratiche di sicurezza di base	ES.5	ES.5
AWS Migliori pratiche di sicurezza di base	ES.6	ES.6
AWS Migliori pratiche di sicurezza di base	ES.7	ES.7
AWS Migliori pratiche di sicurezza di base	ES.8	ES.8

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	EventBridge3.	EventBridge3.
AWS Le migliori pratiche di sicurezza di base	EventBridge4.	EventBridge4.
AWS Migliori pratiche di sicurezza di base	FSX.1	FSX.1
AWS Le migliori pratiche di sicurezza di base	GuardDuty1.	GuardDuty.1.
AWS Migliori pratiche di sicurezza di base	IAM.1	IAM.1
AWS Migliori pratiche di sicurezza di base	IAM.2	IAM.2
AWS Migliori pratiche di sicurezza di base	IAM.3	IAM.3
AWS Migliori pratiche di sicurezza di base	IAM.4	IAM.4
AWS Migliori pratiche di sicurezza di base	IAM.5	IAM.5
AWS Migliori pratiche di sicurezza di base	IAM.6	IAM.6

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	IAM.7	IAM.7
AWS Migliori pratiche di sicurezza di base	IAM.8	IAM.8
AWS Migliori pratiche di sicurezza di base	IAM.9	IAM.9
AWS Migliori pratiche di sicurezza di base	SONO 10	IO SONO 10
AWS Le migliori pratiche di sicurezza di base	IAM.11	IAM.11
AWS Migliori pratiche di sicurezza di base	IAM.12	IAM.12
AWS Migliori pratiche di sicurezza di base	IAM.13	IAM.13
AWS Migliori pratiche di sicurezza di base	IAM.14	IAM.14
AWS Migliori pratiche di sicurezza di base	IAM.15	IAM.15
AWS Migliori pratiche di sicurezza di base	IAM.16	IAM.16

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	IAM.17	IAM.17
AWS Migliori pratiche di sicurezza di base	IAM.18	IAM.18
AWS Migliori pratiche di sicurezza di base	IO HO 19 ANNI	IO SONO 19
AWS Le migliori pratiche di sicurezza di base	IAM.21	IAM.21
AWS Migliori pratiche di sicurezza di base	SONO 22	IO SONO 22
AWS Le migliori pratiche di sicurezza di base	Kinesis.1	Kinesis.1
AWS Migliori pratiche di sicurezza di base	KMS.1	KMS.1
AWS Migliori pratiche di sicurezza di base	KMS.2	KMS.2
AWS Migliori pratiche di sicurezza di base	KMS.3	KMS.3
AWS Migliori pratiche di sicurezza di base	KMS.4	KMS.4

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	Lambda.1	Lambda.1
AWS Migliori pratiche di sicurezza di base	Lambda.2	Lambda.2
AWS Migliori pratiche di sicurezza di base	Lambda.3	Lambda.3
AWS Migliori pratiche di sicurezza di base	Lambda.5	Lambda.5
AWS Migliori pratiche di sicurezza di base	Macie.1	Macie.1
AWS Le migliori pratiche di sicurezza di base	MQ.5	MQ.5
AWS Migliori pratiche di sicurezza di base	MQ.6	MQ.6
AWS Migliori pratiche di sicurezza di base	MSK.1	MSK.1
AWS Le migliori pratiche di sicurezza di base	MSK.2	MSK.2
AWS Le migliori pratiche di sicurezza di base	Nettuno.1	Nettuno.1

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Le migliori pratiche di sicurezza di base	Nettuno.2	Nettuno.2
AWS Le migliori pratiche di sicurezza di base	Nettuno.3	Nettuno.3
AWS Le migliori pratiche di sicurezza di base	Nettuno.4	Nettuno.4
AWS Le migliori pratiche di sicurezza di base	Nettuno.5	Nettuno.5
AWS Le migliori pratiche di sicurezza di base	Nettuno.6	Nettuno.6
AWS Le migliori pratiche di sicurezza di base	Nettuno.7	Nettuno.7
AWS Le migliori pratiche di sicurezza di base	Nettuno.8	Nettuno.8
AWS Le migliori pratiche di sicurezza di base	Nettuno.9	Nettuno.9
AWS Le migliori pratiche di sicurezza di base	NetworkFirewall1.	NetworkFirewall.1.
AWS Migliori pratiche di sicurezza di base	NetworkFirewall2.	NetworkFirewall2.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	NetworkFirewall3.	NetworkFirewall3.
AWS Migliori pratiche di sicurezza di base	NetworkFirewall4.	NetworkFirewall4.
AWS Migliori pratiche di sicurezza di base	NetworkFirewall5.	NetworkFirewall5.
AWS Migliori pratiche di sicurezza di base	NetworkFirewall6.	NetworkFirewall6.
AWS Migliori pratiche di sicurezza di base	NetworkFirewall9.	NetworkFirewall9.
AWS Migliori pratiche di sicurezza di base	Opensearch.1	Opensearch.1
AWS Migliori pratiche di sicurezza di base	Opensearch.2	Opensearch.2
AWS Migliori pratiche di sicurezza di base	Opensearch.3	Opensearch.3
AWS Migliori pratiche di sicurezza di base	Opensearch.4	Opensearch.4
AWS Migliori pratiche di sicurezza di base	Opensearch.5	Opensearch.5

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	Opensearch.6	Opensearch.6
AWS Migliori pratiche di sicurezza di base	Opensearch.7	Opensearch.7
AWS Migliori pratiche di sicurezza di base	Opensearch.8	Opensearch.8
AWS Migliori pratiche di sicurezza di base	Ricerca aperta.10	Ricerca aperta.10
AWS Le migliori pratiche di sicurezza di base	PCA.1	PCA.1
AWS Le migliori pratiche di sicurezza di base	RDS.1	RDS.1
AWS Migliori pratiche di sicurezza di base	RDS.2	RDS.2
AWS Migliori pratiche di sicurezza di base	RDS.3	RDS.3
AWS Migliori pratiche di sicurezza di base	RDS.4	RDS.4
AWS Migliori pratiche di sicurezza di base	RDS.5	RDS.5

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	RDS.6	RDS.6
AWS Migliori pratiche di sicurezza di base	RDS.7	RDS.7
AWS Migliori pratiche di sicurezza di base	RDS.8	RDS.8
AWS Migliori pratiche di sicurezza di base	RDS.9	RDS.9
AWS Migliori pratiche di sicurezza di base	RDS.10	RDS.10
AWS Migliori pratiche di sicurezza di base	RDS.11	RDS.11
AWS Migliori pratiche di sicurezza di base	RDS.12	RDS.12
AWS Migliori pratiche di sicurezza di base	RDS.13	RDS.13
AWS Migliori pratiche di sicurezza di base	RDS.14	RDS.14
AWS Migliori pratiche di sicurezza di base	RDS.15	RDS.15

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	RDS.16	RDS.16
AWS Migliori pratiche di sicurezza di base	RDS.17	RDS.17
AWS Migliori pratiche di sicurezza di base	RDS.18	RDS.18
AWS Migliori pratiche di sicurezza di base	RDS.19	RDS.19
AWS Migliori pratiche di sicurezza di base	RDS.20	RDS.20
AWS Migliori pratiche di sicurezza di base	RDS.21	RDS.21
AWS Migliori pratiche di sicurezza di base	RDS.22	RDS.22
AWS Migliori pratiche di sicurezza di base	RDS.23	RDS.23
AWS Migliori pratiche di sicurezza di base	RDS.24	RDS.24
AWS Migliori pratiche di sicurezza di base	RDS.25	RDS.25

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	RDS.26	RIDS.26
AWS Best practice di sicurezza di base	RDS.27	RDS.27
AWS Best practice di sicurezza di base	RDS.34	RDS.34
AWS Best practice di sicurezza di base	RDS.35	RIDS.35
AWS Best practice di sicurezza di base	Redshift.1	Redshift.1
AWS Migliori pratiche di sicurezza di base	Redshift.2	Redshift.2
AWS Migliori pratiche di sicurezza di base	Redshift.3	Redshift.3
AWS Migliori pratiche di sicurezza di base	Redshift.4	Redshift.4
AWS Migliori pratiche di sicurezza di base	Redshift.6	Redshift.6
AWS Migliori pratiche di sicurezza di base	Redshift.7	Redshift.7
AWS Migliori pratiche di sicurezza di base	Redshift.8	Redshift.8
AWS Migliori pratiche di sicurezza di base	Redshift.9	Redshift.9

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	Redshift.10	Redshift.10
AWS Migliori pratiche di sicurezza di base	Percorso 53.2	Percorso 53.2
AWS Le migliori pratiche di sicurezza di base	S3.1	S3.1
AWS Migliori pratiche di sicurezza di base	S3.2	S3.2
AWS Migliori pratiche di sicurezza di base	S3.3	S3.3
AWS Migliori pratiche di sicurezza di base	S3.4	S3.4
AWS Migliori pratiche di sicurezza di base	S3.5	S3.5
AWS Migliori pratiche di sicurezza di base	S3.6	S3.6
AWS Migliori pratiche di sicurezza di base	S3.7	S3.7
AWS Migliori pratiche di sicurezza di base	S3.8	S3.8

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	S3.9	S3.9
AWS Migliori pratiche di sicurezza di base	S3.11	S3.11
AWS Migliori pratiche di sicurezza di base	S3.12	S3.12
AWS Migliori pratiche di sicurezza di base	S3.13	S3.13
AWS Migliori pratiche di sicurezza di base	S3.14	S3.14
AWS Migliori pratiche di sicurezza di base	S3.15	S3.15
AWS Migliori pratiche di sicurezza di base	S3.17	S3.17
AWS Migliori pratiche di sicurezza di base	S3.19	S3.19
AWS Migliori pratiche di sicurezza di base	S3.19	S3.20
AWS Migliori pratiche di sicurezza di base	SageMaker1.	SageMaker.1.

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	SageMaker2.	SageMaker2.
AWS Migliori pratiche di sicurezza di base	SageMaker3.	SageMaker3.
AWS Migliori pratiche di sicurezza di base	SecretsManager1.	SecretsManager.1.
AWS Migliori pratiche di sicurezza di base	SecretsManager2.	SecretsManager2.
AWS Migliori pratiche di sicurezza di base	SecretsManager3.	SecretsManager3.
AWS Migliori pratiche di sicurezza di base	SecretsManager4.	SecretsManager4.
AWS Migliori pratiche di sicurezza di base	SNS.1	SNS.1
AWS Migliori pratiche di sicurezza di base	SNS.2	SNS.2
AWS Migliori pratiche di sicurezza di base	SQS.1	SQS.1
AWS Migliori pratiche di sicurezza di base	SSM.1	SSM.1

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	SSM.2	SSM.2
AWS Migliori pratiche di sicurezza di base	SSM.3	SSM.3
AWS Migliori pratiche di sicurezza di base	SSM.4	SSM.4
AWS Migliori pratiche di sicurezza di base	StepFunctions1.	StepFunctions.1.
AWS Migliori pratiche di sicurezza di base	WAF.1	WAF.1
AWS Migliori pratiche di sicurezza di base	WAF.2	WAF.2
AWS Migliori pratiche di sicurezza di base	WAF.3	WAF.3
AWS Migliori pratiche di sicurezza di base	WAF.4	WAF.4
AWS Migliori pratiche di sicurezza di base	WAF.6	WAF.6
AWS Migliori pratiche di sicurezza di base	WAF.7	WAF.7

Standard di sicurezza	Parola chiave supportata in Gestione audit (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
AWS Migliori pratiche di sicurezza di base	WAF.8	WAF.8
AWS Migliori pratiche di sicurezza di base	WAF.10	WAF.10
AWS Migliori pratiche di sicurezza di base	WAF.11	WAF.11
AWS Le migliori pratiche di sicurezza di base	WAF.12	WAF.12

Risorse aggiuntive

- Per trovare assistenza sui problemi di raccolta delle prove per questo tipo di origine dati, consulta. La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub
- Per creare un controllo personalizzato utilizzando questo tipo di origine dati, vedereCreazione di un controllo personalizzato in AWS Audit Manager.
- Per creare un framework personalizzato che utilizzi il tuo controllo personalizzato, consultaCreazione di un framework personalizzato in AWS Audit Manager.
- Per aggiungere il controllo personalizzato a un framework personalizzato esistente, vedereModifica di un framework personalizzato in AWS Audit Manager.

AWS Chiamate API supportate da AWS Audit Manager

È possibile utilizzare Audit Manager per acquisire istantanee del proprio AWS ambiente come prova per gli audit. Quando crei o modifichi un controllo personalizzato, puoi specificare una o più chiamate

AWS API come mappatura della fonte di dati per la raccolta delle prove. Audit Manager effettua quindi chiamate API alle risorse pertinenti Servizi AWS e raccoglie un'istantanea dei dettagli di configurazione per le AWS risorse.

Per ogni risorsa che rientra nell'ambito di una chiamata API, Gestione audit acquisisce un'istantanea della configurazione e la converte in prove. Ciò si traduce in una prova per risorsa, anziché una prova per chiamata API.

Ad esempio, se la chiamata API `ec2_DescribeRouteTables` acquisisce istantanee di configurazione da cinque tabelle di routing, otterrai un totale di cinque prove per la singola chiamata API. Ogni prova è un'istantanea della configurazione di una singola tabella di routing.

Argomenti

Punti chiave

Chiamate API impaginate

Molti Servizi AWS raccolgono e archiviano una grande quantità di dati. Di conseguenza, quando una chiamata API `list`, `describe`, o `get` tenta di restituire i dati, i risultati possono essere molti. Se la quantità di dati è troppo grande per essere restituita in un'unica risposta, i risultati possono essere suddivisi in parti più gestibili utilizzando l'impaginazione. In tal modo i risultati vengono suddivisi in "pagine" di dati, semplificando la gestione delle risposte.

Alcuni Chiamate API supportate per fonti di dati di controllo personalizzate sono impaginati. Ciò significa che restituiscono inizialmente risultati parziali e richiedono richieste successive per restituire l'intero set di risultati. Ad esempio, l'operazione Amazon RDS DescribeDBInstances restituisce fino a 100 istanze alla volta e sono necessarie richieste successive per restituire la pagina successiva di risultati.

A partire dall'8 marzo 2023, Gestione audit supporta le chiamate API impaginate come fonte di dati per la raccolta di prove. In precedenza, se una chiamata API impaginata veniva utilizzata come fonte di dati, nella risposta API veniva restituito solo un sottoinsieme delle risorse (fino a 100 risultati). Ora,

Gestione audit richiama l'operazione API impaginata più volte e ottiene ogni pagina di risultati fino alla restituzione di tutte le risorse. Per ogni risorsa, Gestione audit acquisisce quindi un'istantanea della configurazione e la salva come prova. Poiché il set completo di risorse è ora incluso nella risposta dell'API, è probabile che noterai un aumento della quantità di prove raccolte dopo l'8 marzo 2023.

Gestione audit gestisce automaticamente l'impaginazione delle chiamate API. Se crei un controllo personalizzato che utilizza una chiamata API impaginata come origine dati, non è necessario specificare alcun parametro di impaginazione.

Chiamate API supportate per fonti di dati di controllo personalizzate

Nei controlli personalizzati, puoi utilizzare qualsiasi delle seguenti chiamate API come origine dati. Audit Manager può quindi utilizzare queste chiamate API per raccogliere prove sull' AWS utilizzo da parte dell'utente.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
acm_ GetAccountConfiguration	Raccogli uno snapshot delle opzioni di configurazione dell'account associate al tuo Account AWS.
acm_ ListCertificates	Recupera un elenco di ARN di certificati e nomi di dominio.
scalabilità automatica_ DescribeAutoScalingGroups	Raccogli un'istantanea dei gruppi Auto Scaling presenti nel tuo. Account AWS
backup_ ListBackupPlans	Recupera un elenco di tutti i piani di backup attivi nel tuo. Account AWS
bedrock_ GetModelInvocationLoggingConfiguration	Raccogli un'istantanea dei valori di configurazione correnti per la registrazione delle invocazioni dei modelli nel tuo. Account AWS
cloudfront_ ListDistributions	Recupera un elenco di tutte le distribuzioni presenti nel tuo. Account AWS

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
cloudtrail_ DescribeTrails	Raccogli uno snapshot delle impostazioni per uno o più percorsi associati alla Regione corrente per il tuo Account AWS.
sentiero nuvoloso_ ListTrails	Recupera un elenco dei percorsi presenti nel tuo. Account AWS
cloudwatch_ DescribeAlarms	Raccogli uno snapshot di configurazione degli allarmi utilizzati per il tuo Account AWS.
config_ DescribeC onfigRules	Recupera i dettagli sulle tue AWS Config regole.
config_ DescribeD eliveryChannels	Raccogli uno snapshot di configurazione per i canali di distribuzione nel tuo Account AWS.
connessione diretta_ DescribeD irectConnectGatewa ys	Recupera un elenco di tutti i tuoi gateway. AWS Direct Connect
directconnect_ DescribeVirtualGat eways	Recupera un elenco dei gateway virtuali privati di proprietà del tuo Account AWS.
docdb_ DescribeC ertificates	Raccogli un elenco di certificati per il tuo Account AWS.
docdb_describeDB ClusterParameterGr oups	Raccogli un elenco di descrizioni `DBClusterParameterGroup` per il tuo Account AWS.
docdb_Des cribeDBInstances	Raccogli informazioni sulle istanze Amazon DynamoDB con provisioning nel tuo Account AWS.
cloudwatch_ DescribeAlarms	Raccogli informazioni sugli allarmi del tuo. Account AWS

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
cloudtrail_ DescribeTrails	Raccogli un'istantanea delle impostazioni per uno o più percorsi associati al tuo Account AWS
dynamodb_ DescribeTable	Raccogli snapshot di configurazione per le tabelle DynamoDB nel tuo Account AWS. Quando utilizzi questa API come origine dati, non è necessario fornisca il nome di una tabella DynamoDB specifica. Al contrario, Gestione audit utilizza l'operazione `ListTables` per elencare tutte le tabelle. Per ogni tabella elencata, Gestione audit esegue quindi l'operazione `DescribeTable` per generare prove per quella risorsa.
dinamodb_ ListBackups	Recupera un elenco dei backup DynamoDB associati al tuo Account AWS.
dinamodb_ ListTables	Recupera un elenco di tutti i nomi di tabella associati al tuo Account AWS e all'endpoint corrente.
ec2_ DescribeAddresses	Raccogli uno snapshot degli indirizzi IP elastici.
ec2_ DescribeCustomerGateways	Raccogli uno snapshot dei gateway VPN dei clienti.
ec2_ DescribeEgressOnlyInternetGateways	Raccogli uno snapshot dei gateway Internet di sola uscita.
ec2_ DescribeFlowLogs	Raccogli uno snapshot dei log di flusso.
ec2_ DescribeInstances	Raccogli uno snapshot delle istanze.
ec2_ DescribeInternetGateways	Raccogli uno snapshot dei gateway Internet.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Raccogli una descrizione delle associazioni tra i gruppi di interfacce virtuali e le tabelle di routing del gateway locale nella tua. Account AWS
ec2_ DescribeLocalGateways	Raccogli uno snapshot dei gateway locali.
ec2_ DescribeLocalGatewayVirtualInterfaces	Raccogli uno snapshot delle interfacce virtuali del gateway locale.
ec2_ DescribeNatGateways	Raccogli uno snapshot dei gateway NAT.
ec2_ DescribeNetworkAcls	Raccogli uno snapshot delle liste di controllo degli accessi alla rete (ACL).
ec2_ DescribeRouteTables	Raccogli uno snapshot delle tabelle di routing.
ec2_ DescribeSecurityGroups	Raccogli uno snapshot dei gruppi di sicurezza.
ec2_ DescribeSecurityGroupRules	Raccogli un'istantanea di una o più regole del tuo gruppo di sicurezza.
ec2_ DescribeTransitGateways	Raccogli uno snapshot dei gateway di transito.
ec2_ DescribeVolumes	Raccogli uno snapshot dei tuoi endpoint VPC.
ec2_ DescribeVpcs	Raccogli uno snapshot dei VPC.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
ec2_ DescribeVpcEndpoints	Raccogli uno snapshot dei tuoi endpoint VPC.
ec2_ DescribeVpcEndpointConnections	Raccogli un'istantanea delle connessioni degli endpoint VPC ai tuoi servizi endpoint VPC, inclusi tutti gli endpoint in attesa di accettazione.
ec2_ DescribeVpcEndpointServiceConfigurations	Raccogli un'istantanea delle configurazioni del servizio endpoint VPC nel tuo. Account AWS
ec2_ DescribeVpcPeeringConnections	Raccogli uno snapshot delle tue connessioni VPN.
ec2_ DescribeVpnConnections	Raccogli uno snapshot delle tue connessioni VPN.
ec2_ DescribeVpnGateways	Raccogli uno snapshot dei tuoi gateway privati virtuali.
ec2_ GetEbsDefaultKmsKeyId	Raccogli un'istantanea della crittografia EBS predefinita AWS KMS key per la tua Account AWS regione corrente.
ec2_ GetEbsEncryptionByDefault	Descrivi se la crittografia EBS è abilitata per impostazione predefinita per il tuo Account AWS nella Regione corrente.
ecs_ DescribeClusters	Raccogli uno snapshot dei cluster ECS.
eks_ DescribeAddonVersions	Raccogli uno snapshot delle versioni del componente aggiuntivo.
elastica_ DescribeCacheClusters	Raccogli uno snapshot dei cluster con provisioning.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
elasticache_ DescribeS erviceUpdates	Raccogli un'istantanea degli aggiornamenti del servizio per Amazon ElastiCache.
elasticfilesystem_ DescribeA ccessPoints	Raccogli un'istantanea dei punti di accesso Amazon EFS nel tuo Account AWS.
elasticfilesystem_ DescribeFileSystem s	Raccogli uno snapshot dei tuoi file system Amazon EFS.
bilanciamento del carico elastico v2_ DescribeL oadBalancers	Raccogli un'istantanea dei sistemi di bilanciamento del carico del tuo. Account AWS
elasticloadbalanci ngv2_Desc ribeSSLPolicies	Raccogli uno snapshot delle policy utilizzate per la negoziazione SSL.
elasticloadbalanci ng v2_ DescribeT argetGroups	Raccogli uno snapshot dei tuoi gruppi target ELB.
elasticmap reduce_ ListSecurityConfig urations	Recupera un elenco delle configurazioni di sicurezza visibili al tuo Account AWS, insieme alle date e gli orari di creazione e ai relativi nomi.
eventi_ ListConne ctions	Recupera un elenco delle EventBridge connessioni Amazon nel tuo Account AWS.
eventi_ ListEvent Buses	Recupera un elenco dei bus di EventBridge eventi Amazon presenti nel tuo sito Account AWS, inclusi il bus eventi predefinito, gli event bus personali zzati e gli event bus dei partner.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
eventi_ ListEventSources	Recupera un elenco delle origini eventi partner che sono state condivise con il tuo Account AWS.
eventi_ ListRules	Recupera un elenco delle tue EventBridge regole Amazon.
manichetta antincendio_ ListDeliveryStreams	Recupera un elenco dei tuoi flussi di distribuzione.
fsx_ DescribeFileSystems	Raccogli uno snapshot dei file system di proprietà del tuo Account AWS.
servizio di guardia_ ListDetectors	Recupera un elenco delle risorse del `detectorIds` tuo GuardDuty rilevatore Amazon.
sono_ GenerateCredentialReport	Genera un report sulle credenziali per il tuo Account AWS.
sono_ GetAccountPasswordPolicy	Raccogli uno snapshot della policy sulle password per il tuo Account AWS.
sono_ GetAccountSummary	Raccogli uno snapshot dell'utilizzo dell'entità IAM e delle quote IAM nel tuo Account AWS.
sono_ ListGroups	Recupera un elenco dei gruppi IAM associati a un prefisso di percorso disponibile nel tuo. Account AWS
ID iam_ ListOpenConnectProviders	Recupera un elenco degli oggetti risorsa del provider IAM OpenID Connect (OIDC) definiti nel tuo Account AWS.
sono_ ListPolicies	Recupera un elenco di tutte le policy gestite disponibili nel tuo Account AWS, incluse le policy gestite definite dal cliente e tutte le policy gestite da AWS.
sono_ ListRoles	Recupera un elenco dei ruoli IAM associati a un prefisso di percorso disponibile nel tuo. Account AWS

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
iam_ListSAMLProviders	Recupera un elenco degli oggetti risorsa del provider SAML definiti in IAM nel tuo Account AWS.
iam_ ListUsers	Recupera un elenco degli utenti IAM presenti nel tuo. Account AWS
dispositivi iam_ MFA ListVirtual	Recupera un elenco dei dispositivi MFA virtuali definiti nel tuo Account AWS.
kafka_ ListClusters	Recupera un elenco dei cluster Amazon MSK presenti nel tuo. Account AWS
kafka_ ListKafka Versions	Recupera un elenco degli oggetti versione di Apache Kafka nel tuo Account AWS.
cinesi_ ListStreams	Recupera un elenco dei tuoi flussi di dati Kinesis.
kms_ GetKeyPolicy	Gestione audit utilizza questa API per raccogliere uno snapshot delle policy della chiave per le AWS KMS keys nel tuo Account AWS. Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di una specifica. AWS KMS key Al contrario, Gestione audit utilizza l'operazione `ListKeys` per elencare tutte le chiavi KMS. Per ogni chiave KMS elencata, Gestione audit esegue quindi l'operazione `GetKeyPolicy` per generare prove per quella risorsa.
kms_ GetKeyRotationStatus	Audit Manager utilizza questa API per raccogliere un'istantanea del fatto che la rotazione automatica sia abilitata per il AWS KMS keys tuo Account AWS. Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di una specifica AWS KMS key. Al contrario, Gestione audit utilizza l'operazione `ListKeys` per elencare tutte le chiavi KMS. Per ogni chiave KMS elencata, Gestione audit esegue quindi l'operazione `GetKeyRotationStatus` per generare prove per quella risorsa.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
kms_ ListKeys	Recupera un elenco di quelli presenti nel AWS KMS keys tuo. Account AWS
lambda_ ListFunctions	Recupera un elenco di funzioni Lambda nel Account AWS tuo, con la configurazione specifica della versione di ciascuna.
rds_DescribeDBClusters	Raccogli uno snapshot dei cluster Amazon Aurora DB e dei cluster DB Multi-AZ esistenti nel tuo. Account AWS
rds_DescribeDBInstances	Raccogli uno snapshot delle istanze RDS con provisioning nel tuo Account AWS.
rds_ DescribeDbInstanceAutomatedBackups	Raccogli un'istantanea dei backup per le istanze correnti ed eliminate nel tuo. Account AWS
rds_ DescribeDbSecurityGroups	Raccogli un'istantanea del DB nel tuo. SecurityGroups Account AWS
redshift_ DescribeClusters	Raccogli uno snapshot dei cluster Amazon Redshift con provisioning nel tuo Account AWS.
s3_ GetBucketEncryption	Raccogli uno snapshot che mostri la configurazione di crittografia predefinita per i tuoi bucket S3. Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di uno specifico bucket S3. Al contrario, Gestione audit utilizza l'operazione `ListBuckets` per elencare tutti i bucket. Per ogni bucket elencato, Gestione audit esegue quindi l'operazione `GetBucketEncryption` per generare prove per quella risorsa. Audit Manager può fornire lo stato di crittografia solo per i bucket creati durante Regione AWS la valutazione. Se hai bisogno di vedere lo stato di crittografia di tutti i tuoi bucket S3 su più bucket Regioni AWS, ti consigliamo di creare una valutazione in ognuno dei Regione AWS quali hai un bucket S3.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
s3_ ListBuckets	Recupera un elenco dei bucket S3 presenti nel tuo. Account AWS
sagemaker_ ListAlgorithms	Recupera un elenco degli algoritmi di apprendimento automatico presenti nel tuo. Account AWS
sagemaker_ ListDomains	Recupera un elenco dei domini nel tuo. Account AWS
sagemaker_ ListEndpoints	Recupera un elenco degli endpoint nel tuo. Account AWS
sagemaker_ ListEndpointConfigs	Recupera un elenco delle configurazioni degli endpoint nel tuo. Account AWS
sagemaker_ ListFlowDefinitions	Recupera un elenco delle definizioni di flusso nel tuo. Account AWS
sagemaker_ ListHumanTaskUis	Recupera un elenco delle interfacce per le attività umane nel tuo. Account AWS
sagemaker_ ListLabelingJobs	Recupera un elenco dei lavori di etichettatura disponibili nel tuo. Account AWS
sagemaker_ ListModels	Recupera un elenco dei modelli presenti nel tuo. Account AWS
sagemaker _ ListModel BiasJobDefinitions	Recupera un elenco delle definizioni del lavoro basato sul modello nel tuo. Account AWS
sagemaker_ ListModelCards	Recupera un elenco delle schede modello presenti nel tuo. Account AWS
sagemaker_ ListModelQualityJo bDefinitions	Recupera un elenco delle definizioni dei lavori di monitoraggio della qualità dei modelli nel tuo. Account AWS

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
sagemaker_ ListMonitoringAlerts	Recupera un elenco degli avvisi per un determinato programma di monitoraggio.
sagemaker_ ListMonitoringSchedules	Recupera un elenco di tutti i programmi di monitoraggio presenti nel tuo. Account AWS
sagemaker_ ListTrainingJobs	Recupera un elenco di lavori di formazione nel tuo. Account AWS
sagemaker_ ListUserProfiles	Recupera un elenco di profili utente nel tuo. Account AWS
secretsmanager_ ListSecrets	Recupera un elenco dei segreti archiviati nel tuo file Account AWS, esclusi i segreti contrassegnati per l'eliminazione.
sns_ ListTopics	Recupera un elenco degli argomenti SNS nel tuo. Account AWS
sqs_ ListQueues	Recupera un elenco delle code SQS presenti nel tuo. Account AWS
waf-regional_ ListWebAcls	Recupera un elenco degli oggetti WebACLSummary per il tuo. Account AWS
waf-regional_ ListRules	Recupera un elenco degli oggetti per il tuo. RuleSummary Account AWS
waf_ ListRuleGroups	Recupera un elenco degli RuleGroupSummaryoggetti per i gruppi di regole del tuo. Account AWS
waf_ ListRules	Recupera un elenco degli RuleSummaryoggetti per il tuo. Account AWS
waf_ ListWebAcls	Recupera un elenco degli oggetti WebACLSummary per il tuo. Account AWS

Chiamate API utilizzate nel framework standard AWS License Manager

Nel framework standard AWS License Manager, Gestione audit utilizza un'attività personalizzata chiamata `GetLicenseManagerSummary` per raccogliere prove. Questa attività richiama le seguenti tre API di License Manager:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

I dati restituiti vengono quindi convertiti in prove e allegati ai controlli pertinenti della valutazione.

Esempio

Supponiamo che tu utilizzi due prodotti con licenza (SQL Service 2017 e Oracle Database Enterprise Edition). Innanzitutto, l'`GetLicenseManagerSummary`attività richiama l'ListLicenseConfigurationsAPI, che fornisce dettagli sulle configurazioni delle licenze nell'account. Successivamente, aggiunge dati contestuali aggiuntivi per ogni configurazione di licenza ListUsageForLicenseConfigurationchiamando and. ListAssociationsForLicenseConfiguration Infine, converte i dati di configurazione della licenza in prove e li allega ai rispettivi controlli nel framework (4.5 - Licenza gestita dal cliente per SQL Server 2017 e 3.0.4 - Licenza gestita dal cliente per Oracle Database Enterprise Edition).

Se utilizzi un prodotto concesso in licenza che non è coperto da nessuno dei controlli del framework, i dati di configurazione della licenza vengono allegati come prova al seguente controllo: 5.0 - Licenza gestita dal cliente per altre licenze.

Risorse aggiuntive

- Per assistenza sui problemi di raccolta delle prove per questo tipo di origine dati, consultaLa mia valutazione non sta raccogliendo prove dei dati di configurazione per una chiamata AWS API.
- Per creare un controllo personalizzato utilizzando questo tipo di origine dati, vedereCreazione di un controllo personalizzato in AWS Audit Manager.
- Per creare un framework personalizzato che utilizzi il tuo controllo personalizzato, consultaCreazione di un framework personalizzato in AWS Audit Manager.
- Per aggiungere il controllo personalizzato a un framework personalizzato esistente, vedereModifica di un framework personalizzato in AWS Audit Manager.

AWS CloudTrail nomi di eventi supportati da AWS Audit Manager

È possibile utilizzare Audit Manager per acquisire eventi di AWS CloudTrail gestione ed eventi di servizio globali come prove per gli audit. Quando si crea o si modifica un controllo personalizzato, è possibile specificare uno o più nomi di CloudTrail eventi come mappatura dell'origine dati per la raccolta delle prove. Audit Manager filtra quindi CloudTrail i log in base alle parole chiave scelte e importa i risultati come prove dell'attività dell'utente.

> **Note**
>
> Gestione audit acquisisce solo eventi di gestione ed eventi di servizio globali. Gli eventi relativi ai dati e gli eventi di approfondimento non sono disponibili come prove. Per ulteriori informazioni sui diversi tipi di CloudTrail eventi, consulta CloudTrail i concetti nella Guida per l'AWS CloudTrail utente.

In eccezione a quanto sopra, i seguenti CloudTrail eventi non sono supportati da Audit Manager:

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- video di kinesis_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

A partire dall'11 maggio 2023, Audit Manager non supporta più CloudTrail gli eventi di sola lettura come parole chiave per la raccolta delle prove. Abbiamo rimosso un totale di 3.135 parole chiave di sola lettura. Poiché sia i clienti che Servizi AWS effettuano chiamate di lettura alle API, gli eventi di sola lettura sono rumorosi. Di conseguenza, le parole chiave di sola lettura raccolgono molte prove che non sono affidabili o pertinenti per gli audit. Le parole chiave di sola lettura includono `List` e `Describe` le chiamate `Get` API (ad esempio GetObjecte ListBucketsper Amazon S3). Se stavi utilizzando una di queste parole chiave per la raccolta delle prove, non devi compiere alcuna azione. Le parole chiave sono state rimosse automaticamente dalla console Gestione audit e dalle valutazioni e le prove per queste parole chiave non vengono più raccolte.

Risorse aggiuntive

- Per ricevere assistenza sui problemi di raccolta delle prove per questo tipo di origine dati, consulta. La mia valutazione non sta raccogliendo prove dell'attività degli utenti da AWS CloudTrail
- Per creare un controllo personalizzato utilizzando questo tipo di origine dati, vedereCreazione di un controllo personalizzato in AWS Audit Manager.
- Per creare un framework personalizzato che utilizzi il tuo controllo personalizzato, consultaCreazione di un framework personalizzato in AWS Audit Manager.
- Per aggiungere il controllo personalizzato a un framework personalizzato esistente, vedereModifica di un framework personalizzato in AWS Audit Manager.

Configurazione AWS Audit Manager con le impostazioni consigliate

Prima di iniziare a utilizzare Audit Manager, è importante completare le seguenti attività di configurazione.

Questo capitolo illustrerà i prerequisiti, la configurazione dell'account, le autorizzazioni utente e i passaggi necessari per abilitare e configurare Audit Manager con le funzionalità e le integrazioni consigliate. Dopo aver completato queste attività, sarai pronto per utilizzare Audit Manager e iniziare a semplificare le tue attività di audit e conformità.

Indice

Prerequisiti per la configurazione AWS Audit Manager

Prima di poterlo utilizzare AWS Audit Manager, devi assicurarti di aver impostato correttamente le tue autorizzazioni Account AWS e quelle degli utenti.

Questa pagina descrive i passaggi necessari per creare un Account AWS (se necessario), configurare un utente amministrativo e concedere le autorizzazioni necessarie per accedere e abilitare l'Audit Manager.

Attività

1. Iscrivetevi per un Account AWS
2. Crea un utente con accesso amministrativo
3. Aggiungi le autorizzazioni necessarie per accedere e abilitare Gestione audit

> **Important**
>
> Se hai già configurato un IAM, puoi saltare le attività 1 AWS e 2. Tuttavia, è necessario completare l'attività 3 per assicurarsi di disporre delle autorizzazioni necessarie per configurare Audit Manager.

Iscrivetevi per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti 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.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Aggiungi le autorizzazioni necessarie per accedere e abilitare Gestione audit

È necessario fornire agli utenti le autorizzazioni necessarie per abilitare Gestione audit.
Per gli utenti che necessitano dell'accesso completo a Audit Manager, utilizza la policy AWSAuditManagerAdministratorAccessgestita. Si tratta di una politica AWS gestita disponibile nella tua Account AWS azienda ed è la politica consigliata per gli amministratori di Audit Manager.

> **Tip**
>
> Come best practice in materia di sicurezza, ti consigliamo di iniziare con le policy AWS gestite e poi passare alle autorizzazioni con privilegi minimi. AWS le politiche gestite concedono le autorizzazioni per molti casi d'uso comuni. Tuttavia, tieni presente che, poiché le policy AWS gestite sono disponibili per l'uso da parte di tutti i AWS clienti, potrebbero non concedere le autorizzazioni con il minimo privilegio per i tuoi casi d'uso specifici. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSnellaGuida per l'utente AWS Identity and Access Management .

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

- Utenti e gruppi in: AWS IAM Identity Center

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

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

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

Passaggi successivi

Ora che hai configurato Account AWS e concesso le autorizzazioni richieste, sei pronto per abilitare Audit Manager. Per step-by-step istruzioni, consultaAbilitazione AWS Audit Manager.

Abilitazione AWS Audit Manager

Ora che hai completato i prerequisiti per la configurazione di Audit Manager, puoi abilitare il servizio nel tuo AWS ambiente.

In questa pagina imparerai come abilitare Audit Manager utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager. Scegli il metodo più adatto alle tue esigenze e segui i passaggi corrispondenti per rendere operativo Audit Manager.

Prerequisiti

Assicurati di aver completato tutte le attività descritte inPrerequisiti per la configurazione AWS Audit Manager.

Procedura

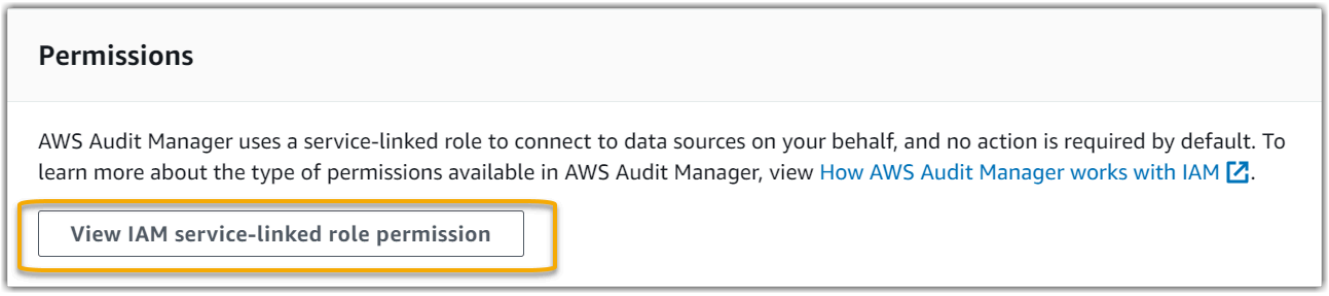
È possibile abilitare Audit Manager utilizzando AWS Management Console, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

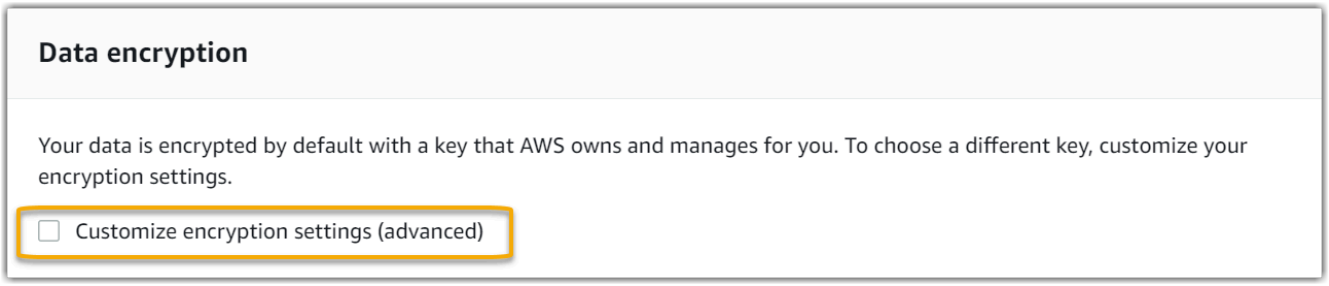
Per abilitare Gestione audit tramite la console

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Usa le credenziali della tua identità IAM per accedere.
3. Scegliere Set up (Configura) AWS Audit Manager.

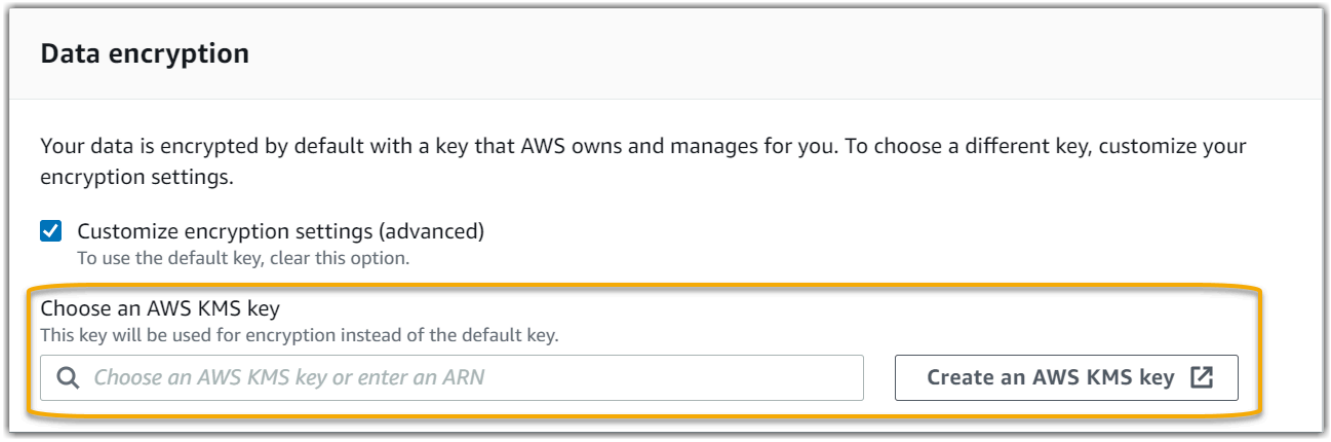
4. In Autorizzazioni, non è richiesta alcuna azione. Ciò perché Gestione audit utilizza un ruolo collegato al servizio per connettersi alle origini dati per conto tuo. Puoi rivedere il ruolo collegato ai servizi scegliendo l'autorizzazione Visualizza il ruolo collegato ai servizi IAM.



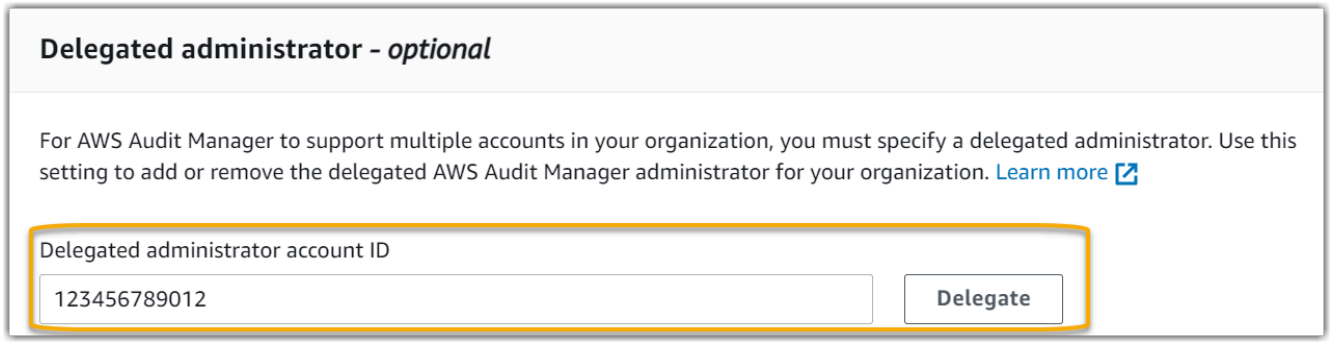
5. In Crittografia dei dati, l'opzione predefinita prevede che Audit Manager crei e gestisca AWS KMS key e archivia i dati in modo sicuro.



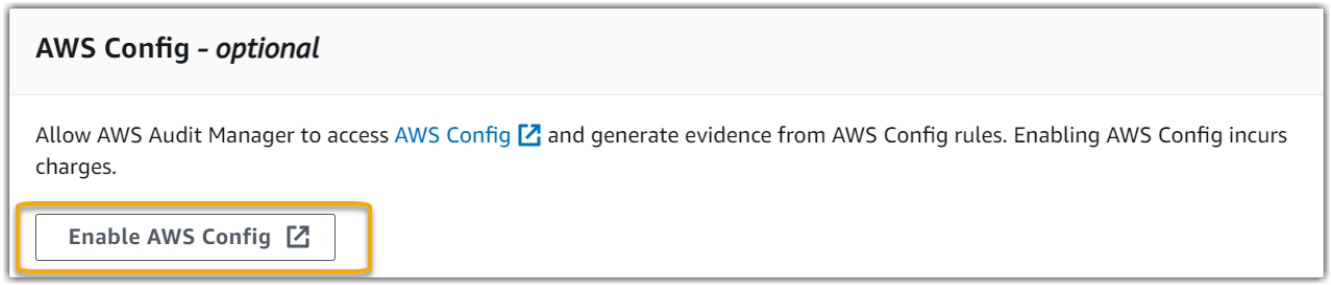
Se desideri utilizzare la tua chiave gestita dal cliente per crittografare i dati in Gestione audit, seleziona la casella di controllo accanto a Personalizza le impostazioni di crittografia (avanzate). Puoi selezionare una chiave KMS esistente o crearne una nuova.



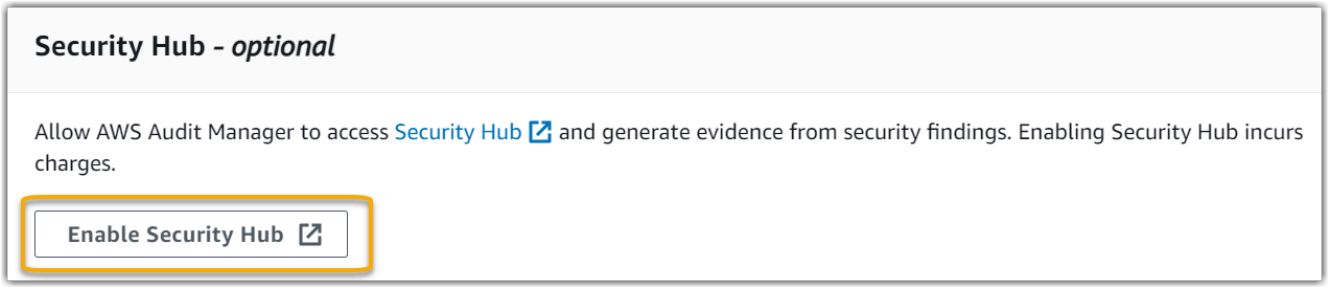
6. (Facoltativo) In Amministratore delegato: facoltativo, è possibile specificare un account amministratore delegato se si desidera che Gestione audit esegua valutazioni per più account. Per maggiori informazioni e consigli, consultare Abilita e configura AWS Organizations (opzionale).



7. (Facoltativo) Nella sezione AWS Config «opzionale», ti consigliamo di abilitarla AWS Config per un'esperienza ottimale. Ciò consente a Gestione audit di generare prove utilizzando regole AWS Config . Per istruzioni e impostazioni consigliate, consultaAbilita e configura AWS Config (facoltativo).



8. (Facoltativo) In Security Hub: facoltativo, ti consigliamo di abilitare Security Hub per un'esperienza ottimale. Ciò consente a Gestione audit di generare prove utilizzando i controlli Security Hub. Per istruzioni e impostazioni consigliate, vedereAbilita e configura AWS Security Hub (facoltativo).



9. Scegli Configurazione completa per completare il processo di configurazione.

AWS CLI

Per abilitare Audit Manager utilizzando AWS CLI

Nella riga di comando, esegui il comando register-account utilizzando i seguenti parametri di configurazione:

- `--kms-key` (facoltativo) — Utilizza questo parametro per crittografare i dati di Gestione audit utilizzando la tua chiave gestita dal cliente. Se non specifichi un'opzione qui, Gestione audit crea e gestisce AWS KMS key per tuo conto per l'archiviazione sicura dei tuoi dati.
- `--delegated-admin-account` (facoltativo): utilizza questo parametro per designare l'account di amministratore delegato dell'organizzazione per Gestione audit. Se non si specifica un'opzione qui, non viene registrato alcun amministratore delegato.

Esempio di input (sostituisci il *testo segnaposto* con le tue informazioni):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Esempio di output:

```
{
    "status": "ACTIVE"
}
```

Per ulteriori informazioni sugli strumenti AWS CLI e per istruzioni sull'installazione degli AWS CLI strumenti, vedere quanto segue nella Guida per l'AWS Command Line Interface utente.

- Guida per l'utente dell'interfaccia a riga di comando di AWS
- Guida introduttiva alla AWS Command Line Interface

Audit Manager API

Per abilitare Gestione audit tramite l'API Gestione audit

Utilizzare l'RegisterAccountoperazione con i seguenti parametri di configurazione:

- kmsKey (facoltativo): utilizza questo parametro per crittografare i dati di Gestione audit utilizzando la tua chiave gestita dal cliente. Se non specifichi un'opzione qui, Gestione audit crea e gestisce AWS KMS key per tuo conto per l'archiviazione sicura dei tuoi dati.
- delegatedAdminAccount(opzionale): utilizzare questo parametro per specificare l'account amministratore delegato dell'organizzazione per Audit Manager. Se non ne specifichi uno, non viene registrato alcun amministratore delegato.

Esempio di input (sostituisci il *testo segnaposto* con le tue informazioni):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Esempio di output:

```
{
  "status": "ACTIVE"
}
```

Passaggi successivi

Dopo aver abilitato Audit Manager, ti consigliamo di configurare alcune funzionalità e integrazioni consigliate per un'esperienza ottimale. Per ulteriori informazioni, consulta Abilitazione delle funzionalità consigliate e per Servizi AWSAWS Audit Manager.

Abilitazione delle funzionalità consigliate e per Servizi AWSAWS Audit Manager

Ora che l'hai abilitata AWS Audit Manager, è il momento di configurare le funzionalità e le integrazioni consigliate per ottenere il massimo dal servizio.

Punti chiave

Per un'esperienza ottimale in Gestione audit, consigliamo di configurare e abilitare le seguenti funzionalità Servizi AWS.

Attività

- Imposta le funzionalità consigliate di Gestione audit
- Configura le integrazioni consigliate con altri Servizi AWS
  - Abilita e configura AWS Config (facoltativo)
  - Abilita e configura AWS Security Hub (facoltativo)
  - Abilita e configura AWS Organizations (opzionale)

Imposta le funzionalità consigliate di Gestione audit

Dopo aver abilitato Gestione audit, ti consigliamo di attivare la funzionalità di ricerca delle prove.

Evidence finder fornisce un modo efficace per cercare prove in Gestione audit. Invece di sfogliare cartelle di prove racchiuse in profondità, per trovare ciò che stai cercando puoi utilizzare evidence finder per interrogare rapidamente le prove. Se utilizzi evidence finder come amministratore delegato, puoi cercare prove in tutti gli account dei membri della tua organizzazione.

Utilizzando una combinazione di filtri e raggruppamenti, è possibile restringere progressivamente l'ambito della query di ricerca. Ad esempio, se desideri una visione di alto livello dello stato del sistema, esegui una ricerca ampia e filtra per valutazione, intervallo di date e conformità delle

risorse. Se il tuo obiettivo è correggere una risorsa specifica, puoi eseguire una ricerca ristretta per individuare le prove relative a un controllo o a un ID di risorsa specifico. Dopo aver definito i filtri, puoi raggruppare e visualizzare in anteprima i risultati di ricerca corrispondenti prima di creare un rapporto di valutazione.

Configura le integrazioni consigliate con altri Servizi AWS

Per un'esperienza ottimale in Audit Manager, ti consigliamo vivamente di abilitare quanto segue Servizi AWS:

- AWS Organizations: è possibile utilizzare Organizations per eseguire le valutazioni di Gestione audit su più account e consolidare le prove in un account amministratore delegato.
- AWS Security Hub AWS Config— Quando li abiliti Servizi AWS, possono essere utilizzati come tipo di origine dati per i controlli nelle valutazioni dell'Audit Manager. Gestione audit può quindi riportare i risultati dei controlli di conformità direttamente da questi servizi.

> **Important**
>
> Enabling AWS Config, Security Hub and Organizations è una raccomandazione facoltativa. Tuttavia, se si abilitano questi servizi, è richiesta la seguente configurazione.

Abilita e configura AWS Config (facoltativo)

Molti controlli in Audit Manager vengono utilizzati AWS Config come tipo di origine dati. Per supportare questi controlli, è necessario abilitarli AWS Config su tutti gli account in ognuno dei Regione AWS quali è abilitato Audit Manager. Se Audit Manager tenta di raccogliere prove per i controlli utilizzati AWS Config come tipo di origine dati e le relative AWS Config regole non sono abilitate, non viene raccolta alcuna evidenza per tali controlli.

Audit Manager non gestisce AWS Config per te. Puoi seguire queste fasi per abilitare AWS Config e configurare le impostazioni.

> **Important**
>
> L'abilitazione AWS Config è una raccomandazione facoltativa. Tuttavia, se abiliti AWS Config, sono necessarie le seguenti impostazioni.

Attività da integrare AWS Config con Audit Manager

- Fase 1: Abilita AWS Config
- Fase 2: Configurare AWS Config le impostazioni per l'utilizzo con Audit Manager

Fase 1: Abilita AWS Config

È possibile abilitare AWS Config utilizzando la AWS Config console o l'API. Per istruzioni, consulta Nozioni di base con AWS Config nella Guida per gli sviluppatori di AWS Config .

Fase 2: Configurare AWS Config le impostazioni per l'utilizzo con Audit Manager

Dopo l'attivazione AWS Config, assicurati di abilitare anche AWS Config le regole o di distribuire un pacchetto di conformità per lo standard di conformità correlato al tuo audit. Questa fase garantisce che Gestione audit possa importare i risultati per le regole AWS Config che hai abilitato.

Dopo aver abilitato una AWS Config regola, ti consigliamo di esaminarne i parametri. Quindi, convalida tali parametri in base ai requisiti del framework di conformità prescelto. Se necessario, puoi aggiornare i parametri di una regola in AWS Configper assicurarti che sia in linea con i requisiti del framework. Ciò contribuirà a garantire che le valutazioni raccolgano le prove di verifica della conformità corrette per un determinato framework.

Ad esempio, supponiamo che tu stia creando una valutazione per CIS v1.2.0. Questo framework ha un controllo denominato 1.4: assicurati che le chiavi di accesso vengano ruotate ogni 90 giorni o meno. In AWS Config, la access-keys-rotatedregola ha un `maxAccessKeyAge` parametro con un valore predefinito di 90 giorni. Di conseguenza, la regola è conforme ai requisiti di controllo. Se non utilizzate il valore predefinito, assicuratevi che il valore che state utilizzando sia uguale o superiore ai 90 giorni richiesti dal CIS v1.2.0.

Puoi trovare i dettagli dei parametri predefiniti per ogni regola gestita nella documentazione AWS Config. Per istruzioni su come configurare una regola, consulta Working with AWS Config Managed Rules.

Abilita e configura AWS Security Hub (facoltativo)

Molti controlli in Gestione audit utilizzano Security Hub come tipo di origine dati. Per supportare questi controlli, occorre abilitare Security Hub su tutti gli account in ogni regione in cui è abilitato Gestione audit. Se Gestione audit tenta di raccogliere prove per i controlli che utilizzano Security Hub come

tipo di origine dati e i relativi standard Security Hub non sono abilitati, non viene raccolta alcuna prova per tali controlli.

Gestione audit non gestisce Security Hub per te. Puoi seguire queste fasi per abilitare Security Hub e configurarne le impostazioni.

> **Important**
>
> L'attivazione di Security Hub è un consiglio facoltativo. Tuttavia, se abiliti Security Hub, sono necessarie le seguenti impostazioni.

Attività da integrare AWS Security Hub con Audit Manager

- Fase 1: Abilita AWS Security Hub
- Fase 2: configurazione delle impostazioni Security Hub da utilizzare con Gestione audit
- Fase 3: Configurare le impostazioni Organizations per la propria organizzazione

Fase 1: Abilita AWS Security Hub

Puoi abilitare Security Hub utilizzando sia la console che l'API. Per istruzioni, consulta Configurazione di AWS Security Hubnella Guida per l'utente AWS Security Hub .

Fase 2: configurazione delle impostazioni Security Hub da utilizzare con Gestione audit

Dopo aver abilitato Security Hub, assicurati di eseguire anche la seguente procedura:

- Abilita AWS Config e configura la registrazione delle risorse: Security Hub utilizza AWS Config regole collegate ai servizi per eseguire la maggior parte dei controlli di sicurezza. Per supportare questi controlli, AWS Config deve essere abilitato e configurato per registrare le risorse necessarie per i controlli abilitati in ogni standard abilitato.
- Abilita tutti gli standard di sicurezza: questo passaggio garantisce che Audit Manager possa importare i risultati per tutti gli standard di conformità supportati.
- Attiva l'impostazione dei risultati del controllo consolidato nel Security Hub: questa impostazione è attivata per impostazione predefinita se abiliti Security Hub a partire dal 23 febbraio 2023.

> **Note**
>
> Quando abiliti i risultati consolidati, Security Hub produce un singolo risultato per ogni controllo di sicurezza (anche quando lo stesso controllo viene utilizzato su più standard). Ogni risultato Security Hub viene raccolto come un'unica valutazione delle risorse in Gestione audit. Di conseguenza, i risultati consolidati comportano una diminuzione delle valutazioni totali delle risorse uniche eseguite da Gestione audit per i risultati Security Hub. Per tale motivo, l'utilizzo di risultati consolidati può spesso portare a una riduzione dei costi di utilizzo di Gestione audit. Per ulteriori informazioni sull'utilizzo Security Hub come tipo di origine dati, consulta AWS Security Hub controlli supportati da AWS Audit Manager. Per ulteriori informazioni sui prezzi di Gestione audit, consulta Prezzi di AWS Audit Manager.

Fase 3: Configurare le impostazioni Organizations per la propria organizzazione

Se utilizzi AWS Organizations e desideri raccogliere prove di Security Hub dagli account dei tuoi membri, devi anche eseguire i seguenti passaggi in Security Hub.

Per configurare le impostazioni Security Hub

1. Accedi AWS Management Console e apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/.
2. Utilizzando il tuo account di AWS Organizations gestione, designa un account come amministratore delegato per Security Hub. Per ulteriori informazioni, consulta Designazione di un account amministratore Security Hub nella Guida per l'utente di AWS Security Hub .

   > **Note**
   >
   > Assicurati che l'account amministratore delegato che designi nel Security Hub sia lo stesso che utilizzi in Gestione audit.

3. Utilizzando il tuo account amministratore delegato Organizations, vai a Impostazioni, Account, seleziona tutti gli account, quindi aggiungili come membri selezionando Registrazione automatica. Per maggiori informazioni, consulta Abilitazione di un account membro nell'organizzazione nella Guida per l'utente di AWS Security Hub .

4. Abilita AWS Config per ogni account membro dell'organizzazione. Per maggiori informazioni, consulta Abilitazione di un account membro nell'organizzazione nella Guida per l'utente di AWS Security Hub .
5. Abilita lo standard di sicurezza PCI DSS per ogni account membro dell'organizzazione. Lo standard AWS CIS Foundations Benchmark e lo standard AWS Foundational Best Practices sono già abilitati per impostazione predefinita. Per ulteriori informazioni, consulta Abilitazione di uno standard di sicurezza nella Guida per l'utente AWS Security Hub .

Abilita e configura AWS Organizations (opzionale)

Audit Manager supporta più account tramite l'integrazione con AWS Organizations. Gestione audit può eseguire le valutazioni su più account e consolidare le prove in un account amministratore delegato. L'amministratore delegato dispone delle autorizzazioni per creare e gestire le risorse Gestione audit con l'organizzazione come zona di attendibilità. Solo l'account di gestione può designare un amministratore delegato.

> **Important**
>
> L'abilitazione AWS Organizations è una raccomandazione facoltativa. Tuttavia, se si abilita AWS Organizations, sono necessarie le seguenti impostazioni.

Attività da integrare AWS Organizations con Audit Manager

- Fase 1: Creazione o adesione a un'organizzazione
- Fase 2: abilitazione di tutte le caratteristiche nell'organizzazione
- Fase 3: specificare un amministratore delegato per Gestione audit

Fase 1: Creazione o adesione a un'organizzazione

Se Account AWS non fai parte di un'organizzazione, puoi creare o entrare a far parte di un'organizzazione. Per istruzioni, consulta Creazione e configurazione di un'organizzazione nella Guida per l'utente di AWS Organizations .

Fase 2: abilitazione di tutte le caratteristiche nell'organizzazione

Quindi, abilita tutte le funzionalità nell'organizzazione. Per le istruzioni, consulta la sezione Abilitazione di tutte le funzionalità nell'organizzazione nella Guida per l'utente di AWS Organizations .

Fase 3: specificare un amministratore delegato per Gestione audit

Si consiglia di abilitare Gestione audit utilizzando un account di gestione Organizations e quindi di specificare un amministratore delegato. Successivamente, è possibile utilizzare l'account amministratore delegato per accedere ed eseguire le valutazioni. Come best practice, consigliamo di creare valutazioni solo utilizzando l'account amministratore delegato anziché l'account di gestione.

Per aggiungere o modificare un amministratore delegato dopo aver abilitato Audit Manager, vedere Aggiungere un amministratore delegato eModifica di un amministratore delegato.

Passaggi successivi

Ora che hai configurato Audit Manager con le impostazioni consigliate, sei pronto per iniziare a utilizzare il servizio.

- Per iniziare con la prima valutazione, consultaTutorial per i proprietari degli audit: creazione di una valutazione.
- Per aggiornare le impostazioni in futuro, consultaRevisione e configurazione delle impostazioni AWS Audit Manager.

Iniziare con AWS Audit Manager

Utilizza i step-by-step tutorial in questa sezione per imparare a eseguire operazioni utilizzando. AWS Audit Manager

> **Tip**
>
> I seguenti tutorial sono suddivisi in categorie di destinatari. Scegli il tutorial più adatto a te in base al tuo ruolo di proprietario dell'audit o delegato dell'audit.
>
> - I proprietari dell'audit sono utenti di Gestione audit responsabili della creazione e della gestione delle valutazioni. Nel mondo degli affari, i responsabili degli audit sono in genere professionisti della governance, della gestione del rischio e della conformità (GRC). Nel contesto di Audit Manager, tuttavia, gli individui SecOps o DevOps i team potrebbero anche assumere la persona utente del titolare dell'audit. I proprietari dell'audit possono richiedere l'assistenza di un esperto in materia, noto anche come delegato, per esaminare controlli specifici e convalidare le prove. I proprietari dell'audit devono disporre delle autorizzazioni necessarie per gestire una valutazione.
> - I delegati sono esperti in materia con competenze tecniche o commerciali specializzate. Sebbene non possiedano o gestiscano le valutazioni di Gestione audit, possono comunque contribuire ad esse. I delegati assistono i proprietari degli audit in attività come la convalida delle prove per i controlli che rientrano nella loro area di competenza. I delegati dispongono di autorizzazioni limitate in Gestione audit. Questo perché i proprietari degli audit delegano specifici set di controlli per la revisione e non intere valutazioni.
>
> Per ulteriori informazioni su questi personaggi e su altri concetti di Audit Manager, vedere audit owner e delegate nella Comprensione dei concetti e della terminologia AWS Audit Manager sezione di questa guida.
> Per ulteriori informazioni sulle autorizzazioni IAM consigliate per ogni utente, consulta Politiche consigliate per gli utenti in AWS Audit Manager.

Tutorial Gestione audit

Creazione di una valutazione

Destinatari: proprietari degli audit

Panoramica: segui step-by-step le istruzioni per creare la tua prima valutazione e iniziare subito. Questo tutorial illustra come utilizzare un framework standard per creare una valutazione e iniziare la raccolta automatica di prove.

Revisione di un set di controlli

Destinatari: delegati

Panoramica: assisti il responsabile dell'audit esaminando le prove relative ai controlli che rientrano nella tua area di competenza. Scopri come esaminare i set di controllo e le relative prove, aggiungere commenti, caricare prove e aggiornare lo stato di un controllo.

Tutorial per i proprietari degli audit: creazione di una valutazione

Questo tutorial fornisce un'introduzione a AWS Audit Manager. In questo tutorial, crei una valutazione utilizzandoAWS Audit Manager Framework di esempio. Creando una valutazione, si avvia il processo continuo di raccolta automatica delle prove per i controlli di quel framework.

> **Note**
>
> AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici quadri e regolamenti di conformità. Tuttavia, non viene eseguita la valutazione della conformità. AWS Audit Manager Pertanto, le prove raccolte potrebbero non includere tutte le informazioni sull' AWS utilizzo necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Prerequisiti

Prima di iniziare questo tutorial, assicurati di soddisfare le seguenti condizioni:

- Hai completato tutti i prerequisiti descritti in Configurazione AWS Audit Manager con le impostazioni consigliate. Devi usare la tua console Account AWS e quella della AWS Audit Manager console per completare questo tutorial.
- Alla tua identità IAM vengono concesse le autorizzazioni adeguate per creare e gestire una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager eConsentire l'accesso alla gestione degli utenti a AWS Audit Manager.

- Conosci la terminologia e le funzionalità di Gestione audit. Per una panoramica generale, consulta Che cos'è AWS Audit Manager? e Comprensione dei concetti e della terminologia AWS Audit Manager.

Procedura

Attività

- Fase 1: specificare i dettagli della valutazione
- Fase 2: Specificare Account AWS l'ambito
- Fase 3: Specificare i titolari dell'audit
- Fase 4: Revisione e creazione

Fase 1: specificare i dettagli della valutazione

Per la prima fase, seleziona un framework e fornisci le informazioni di base per la valutazione.

Specificare i dettagli della valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Avvia AWS Audit Manager.
3. Nel banner verde nella parte superiore dello schermo, scegli Inizia con un framework.
4. Scegli il framework che desideri, quindi scegli Crea valutazione dal framework. Per questo tutorial, usa AWS Audit Manager Sample Framework.
5. Nella sezione Nome valutazione, inserisci un nome per la valutazione.
6. (Facoltativo) Nella sezione Descrizione della valutazione, inserisci una descrizione per la valutazione.
7. In Destinazione dei report di valutazione, scegli il bucket S3 in cui desideri salvare i report di valutazione.
8. In Frameworks, conferma che AWS Audit Manager Sample Framework sia selezionato.
9. (Facoltativo) In Tag, scegli Aggiungi nuovo tag per associare un tag alla tua valutazione. Per ogni tag è possibile specificare una chiave e un valore. La chiave di tag è obbligatoria e può essere utilizzata come criterio di ricerca quando cerchi questa valutazione.

10. Seleziona Successivo.

Fase 2: Specificare Account AWS l'ambito

Successivamente, specifica gli AWS account che desideri includere nell'ambito della valutazione.

AWS Audit Manager si integra con AWS Organizations, in modo da poter eseguire una valutazione Audit Manager su più account e consolidare le prove in un account amministratore delegato. Per abilitare Organizations in Gestione audit (se non l'hai già fatto), consulta Abilita e configura AWS Organizations (opzionale) nella pagina Configurazione di questa guida.

> **Note**
>
> Audit Manager può supportare fino a 200 account nell'ambito di una valutazione. Se si tenta di includere più di 200 account, la creazione della valutazione potrebbe non riuscire.

Specificare gli account nell'ambito di applicazione

1. In Account AWS, seleziona Account AWS quello che desideri includere nell'ambito della valutazione.
   - Se hai abilitato Organizations in Audit Manager, vengono elencati più account.
   - Se non hai abilitato Organizations in Audit Manager, viene elencato solo il tuo account corrente.
2. Seleziona Successivo.

Fase 3: Specificare i titolari dell'audit

In questa fase, specifica i proprietari dell'audit per la valutazione. I responsabili dell'audit sono le persone sul posto di lavoro, in genere appartenenti a GRC o ai DevOps team SecOps, responsabili della gestione della valutazione dell'Audit Manager. Consigliamo loro di utilizzare la politica. AWSAuditManagerAdministratorAccess

Specificare i proprietari dell'audit

1. Nella sezione Proprietari dell'audit, scegli i proprietari dell'audit per la tua valutazione. Per trovare altri titolari di audit, utilizza la barra di ricerca per nome o Account AWS.
2. Seleziona Successivo.

Fase 4: Revisione e creazione

Rivedi le informazioni per la valutazione. Per modificare le informazioni relative a una fase, scegli Modifica. Quando hai finito, scegli Crea valutazione per iniziare la raccolta continua di prove.

Dopo aver creato una valutazione, la raccolta delle prove continua finché non modifichi lo stato della valutazione, impostandolo su inattivo. In alternativa, puoi interrompere la raccolta delle prove per un controllo specifico modificando lo stato del controllo e impostandolo su inattivo.

> **Note**
>
> Le prove automatiche sono disponibili 24 ore dopo la creazione della valutazione. Gestione audit raccoglie automaticamente le prove da più origini dati e la frequenza di tale raccolta di prove si basa sul tipo di evidenza. Per ulteriori informazioni sul tagging, consulta Frequenza di raccolta delle provein questa guida.

Risorse aggiuntive

Ti consigliamo di continuare con ulteriori informazioni su concetti e strumenti introdotti in questo tutorial. Puoi farlo consultando le risorse seguenti:

- Revisione dei dettagli della valutazione in AWS Audit Manager— Ti introduce alla pagina dei dettagli della valutazione in cui puoi esplorare i diversi componenti della valutazione.
- Gestione delle valutazioni in AWS Audit Manager – Si basa su questo tutorial e fornisce informazioni dettagliate su concetti e attività relativi a gestione di una valutazione. In questo capitolo, ti consigliamo in particolare di consultare i seguenti argomenti:
  - Come creare una valutazione da un framework diverso
  - Come esaminare le prove contenute in una valutazione e generare un rapporto di valutazione
  - Come modificare lo stato di una valutazione o eliminare una valutazione
- Utilizzo della libreria di framework per gestire i framework in AWS Audit Manager – Presenta la libreria di framework e spiega come creare un framework personalizzato per esigenze di conformità specifiche.
- Utilizzo della libreria di controlli per gestire i controlli in AWS Audit Manager – Presenta la libreria di controlli e spiega come creare un controllo personalizzato da utilizzare nel framework personalizzato.

- Comprensione dei concetti e della terminologia AWS Audit Manager – Fornisce le definizioni dei concetti e della terminologia utilizzati in Gestione audit.
- [Video] Raccolta delle prove e gestione dei dati di audit AWS Audit Manager: mostra il processo di creazione della valutazione descritto in questo tutorial e altre attività come la revisione di un controllo e la generazione di un rapporto di valutazione.

Tutorial per delegati: revisione di un set di controlli

Questo tutorial descrive come rivedere un set di controlli che è stato condiviso con te da un proprietario dell'audit in AWS Audit Manager.

I titolari degli audit utilizzano Audit Manager per creare valutazioni e raccogliere prove per i controlli in tale valutazione. A volte i proprietari degli audit potrebbero avere domande o aver bisogno di assistenza durante la convalida delle prove per un set di controlli. In questa situazione, il proprietario dell'audit può delegare un set di controlli a un esperto in materia per la revisione.

In qualità di delegato, aiuti i responsabili degli audit a esaminare le prove raccolte per verificare i controlli che rientrano nella tua area di competenza.

Prerequisiti

Prima di iniziare questo tutorial, assicurati che siano soddisfatte le seguenti condizioni:

- Il tuo Account AWS è configurato. Per completare questo tutorial, devi utilizzare sia la tua Account AWS console che quella di Audit Manager. Per ulteriori informazioni, consulta Configurazione AWS Audit Manager con le impostazioni consigliate.
- Conosci la terminologia e le funzionalità di Gestione audit. Per una panoramica generale di Gestione audit, consulta Che cos'è AWS Audit Manager? e Comprensione dei concetti e della terminologia AWS Audit Manager.

Procedura

Attività

- Passaggio 1: rivedi le notifiche
- Fase 2: esaminare un set di controlli e le relative prove
- Fase 3. Aggiungi prove manuali (opzionale)

- Fase 4. Aggiungi un commento per un controllo (facoltativo)
- Fase 5: contrassegna un controllo come revisionato (facoltativo)
- Fase 6. Restituisci il set di controlli revisionato al proprietario dell'audit

Passaggio 1: rivedi le notifiche

Inizia accedendo a Audit Manager, dove puoi accedere alle tue notifiche per vedere i set di controllo che ti sono stati delegati per la revisione.

Per rivedere le tue notifiche

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione sinistro, seleziona Notifiche.
3. Nella pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. La tabella delle notifiche include le seguenti informazioni:

Nome	Descrizione
Data	La data in cui il set di controllo è stato delegato.
Valutazione	Il nome della valutazione associata al set di controlli. Puoi scegliere un nome per la valutazione per aprire la pagina dei dettagli della valutazione.
Set di controllo	Il nome del set di controlli che ti è stato delegato per la revisione .
Origine	L'utente o il ruolo che ti ha delegato il set di controllo.
Descrizione	Le istruzioni di revisione fornite dal titolare dell'audit.

> **Tip**
>
> Puoi anche iscriverti a un argomento SNS per ricevere avvisi e-mail quando ti viene assegnato un set di controlli per la revisione. Per ulteriori informazioni, consulta Notifiche in AWS Audit Manager.

Fase 2: esaminare un set di controlli e le relative prove

Il passaggio successivo consiste nel rivedere i set di controlli che il proprietario dell'audit ti ha delegato. Esaminando i controlli e le relative evidenze, puoi stabilire se sono necessarie ulteriori azioni per un controllo. Le azioni aggiuntive possono includere il caricamento manuale di prove aggiuntive per dimostrare la conformità o l'inserimento di un commento su tale controllo.

Revisione di un set di controlli

1. Dalla pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. Quindi identifica quello che desideri esaminare e scegli il nome della valutazione correlata.
2. Nella sezione Controlli della pagina dei dettagli della valutazione, scorri verso il basso fino alla tabella Impostazioni controlli.
3. Nella colonna Controlli raggruppati per set di controlli, espandi il nome di un set di controlli per mostrarne i controlli. Quindi, scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
4. (Facoltativo) Scegli Aggiorna stato del controllo per modificare lo stato del controllo. Durante la revisione, puoi contrassegnare lo stato come In corso di revisione.
5. Consulta le informazioni sul controllo nelle schede Evidence folder, Details, Evidence sources, Comments e Changelog. Per ulteriori informazioni su ciascuna di queste schede e su come comprendere i dati in esse contenuti, consulta. Revisione di un controllo di valutazione in AWS Audit Manager

Per esaminare le prove per un controllo

1. Dalla pagina dei dettagli del controllo, scegli la scheda Cartelle di prove.
2. Passa alla tabella Cartelle di prove, dove viene visualizzato un elenco di cartelle che contengono le prove per quel controllo. Queste cartelle sono organizzate e denominate in base alla data in cui sono state raccolte le prove all'interno di quella cartella.

3. Scegli il nome di una cartella di prove per aprirla. Da qui, puoi consultare un riepilogo di tutte le prove raccolte in quella data. Per comprendere queste informazioni, vedereRevisione di una cartella di prove in AWS Audit Manager.
4. Dalla pagina di riepilogo della cartella delle prove, vai alla tabella Prove. Nella colonna Ora, scegli una voce per aprire ed esaminare i dettagli delle prove raccolte in quel momento. Per comprendere queste informazioni, vedereRevisione delle prove in AWS Audit Manager.

Fase 3. Aggiungi prove manuali (opzionale)

Sebbene raccolga AWS Audit Manager automaticamente le prove per molti controlli, in alcuni casi potrebbe essere necessario fornire prove aggiuntive. In questi casi, puoi aggiungere manualmente le tue prove che ti aiutano a dimostrare la conformità a tale controllo.

Per aggiungere prove manuali a un controllo

Esistono diversi modi per aggiungere prove manuali a un controllo. Puoi importare un file da Amazon S3, caricare un file dal tuo browser o inserire una risposta di testo. Per le istruzioni relative a ciascun metodo, consultaAggiungere prove manuali in AWS Audit Manager.

Fase 4. Aggiungi un commento per un controllo (facoltativo)

Puoi aggiungere commenti per tutti i controlli che esamini. Questi commenti sono visibili al proprietario dell'audit. Ad esempio, puoi lasciare un commento per fornire un aggiornamento sullo stato e confermare di aver risolto eventuali problemi relativi a tale controllo.

Per aggiungere un commento a un controllo

1. Dalla pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. Trova il set di controlli per cui desideri lasciare un commento e scegli il nome della valutazione correlata.
2. Scegli la scheda Controlli, scorri verso il basso fino alla tabella Set di controlli, quindi seleziona il nome di un controllo per aprirlo.
3. Scegli la scheda Commenti.
4. Nella sezione Invia commenti, inserisci il tuo commento nella casella di testo.
5. Scegli Invia commenti per aggiungere il tuo commento. Il tuo commento viene ora visualizzato nella sezione Commenti precedenti della pagina insieme a qualsiasi altro commento relativo a questo controllo.

Fase 5: contrassegna un controllo come revisionato (facoltativo)

La modifica dello stato di un controllo è facoltativa. Tuttavia, ti consigliamo di modificare lo stato di ogni controllo e impostarlo su Revisionato una volta completata la revisione di quel controllo. Indipendentemente dallo stato di ogni singolo controllo, puoi comunque inviare i controlli al proprietario dell'audit.

Per contrassegnare un controllo come revisionato

1. Dalla pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. Trova il set di controlli che contiene il controllo che desideri contrassegnare come revisionato. Pertanto, scegli il nome della valutazione correlata per aprire la pagina dei dettagli della valutazione.
2. Nella sezione Controlli della pagina dei dettagli della valutazione, scorri verso il basso fino alla tabella Impostazioni controlli.
3. Nella colonna Controlli raggruppati per set di controlli, espandi il nome di un set di controlli per mostrarne i controlli. Scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
4. Scegli Aggiorna lo stato del controllo e modifica lo stato impostandolo su Revisionato.
5. Nella finestra pop-up che appare, scegli Aggiorna lo stato del controllo per confermare di aver terminato la revisione del controllo.

Fase 6. Restituisci il set di controlli revisionato al proprietario dell'audit

Quando hai finito di esaminare tutti i controlli, invia il set di controlli al proprietario dell'audit per fargli sapere che hai terminato la revisione.

Per restituire un set di controlli revisionato al proprietario

1. Dalla pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati assegnati. Trova il set di controlli che desideri inviare al proprietario dell'audit e scegli il nome della valutazione correlata.
2. Scorri verso il basso fino alla tabella Set di controlli, seleziona il set di controlli che desideri restituire al proprietario dell'audit e poi scegli Invia per una revisione.
3. Nella finestra pop-up che appare, puoi aggiungere eventuali commenti di alto livello su quel set di controlli prima di scegliere Invia per una revisione.

Dopo aver inviato il controllo al proprietario dell'audit, quest'ultimo può visualizzare tutti i commenti che hai lasciato.

Risorse aggiuntive

Puoi continuare con ulteriori informazioni sui concetti introdotti in questo tutorial. Ecco alcune risorse consigliate:

- Revisione dei dettagli della valutazione in AWS Audit Manager- Presenta la pagina dei dettagli della valutazione, in cui è possibile esplorare i diversi componenti di una valutazione Audit Manager.
- Revisione di un controllo di valutazione in AWS Audit Managere Revisione delle prove in AWS Audit Manager - Fornisce definizioni per aiutarvi a comprendere i controlli e le evidenze di una valutazione.
- Comprensione dei concetti e della terminologia AWS Audit Manager - Fornisce le definizioni dei concetti e della terminologia utilizzati in Gestione audit.

Utilizzo del pannello di controllo Gestione audit

Con il pannello di controllo Gestione audit, puoi visualizzare le prove di non conformità nelle tue valutazioni attive. È un modo comodo e veloce per monitorare le valutazioni, rimanere informati e risolvere i problemi in modo proattivo. Per impostazione predefinita, il pannello di controllo offre una visualizzazione aggregata dall'alto verso il basso di tutte le valutazioni attive. Utilizzando questa visualizzazione, puoi identificare visivamente i problemi nelle tue valutazioni senza dover prima vagliare grandi quantità di prove individuali.

Il pannello di controllo è la prima schermata che viene visualizzata quando si accede alla console Gestione audit. Contiene due widget che mostrano i dati e gli indicatori chiave di prestazione (KPI) più pertinenti per te. Utilizzando un filtro di valutazione, puoi affinare questi dati per concentrarti sugli indicatori chiave di presentazione (KPI) per una valutazione specifica. Da lì, puoi esaminare i raggruppamenti dei domini di controllo per identificare quali controlli presentano il maggior numero di prove di non conformità. Quindi, puoi esplorare i controlli sottostanti per esaminare e risolvere i problemi.

> **Note**
>
> Se sei un utente di Gestione audit per la prima volta o non disponi di valutazioni attive, nel pannello di controllo non viene visualizzato alcun dato. Per iniziare, crea una valutazione. Ciò dà inizio alla raccolta continua di prove. Dopo un periodo di 24 ore, i dati aggregati relativi alle prove inizieranno a comparire nel pannello di controllo. Le sezioni seguenti includono la comprensione e l'interpretazione di questi dati.

Questa pagina comprende i seguenti argomenti:

Argomenti

Concetti e terminologia del pannello di controllo

Questa sezione descrive cose importanti da sapere sul pannello di controllo di Gestione audit prima di iniziare a utilizzarla.

Autorizzazioni e visibilità

Sia i titolari dell'audit che i delegati hanno accesso al pannello di controllo. Ciò significa che entrambe queste persone possono vedere le metriche e gli aggregati per tutte le valutazioni attive nel tuo. Account AWS L'accesso alle stesse informazioni consente a tutto il team di concentrarsi sugli stessi indicatori chiave di presentazione (KPI) e obiettivi.

Filtri

Gestione audit fornisce un livello di pagina the section called "Filtro di valutazione" che puoi applicare a tutti i widget sulla dashboard.

Prove non conformi

Il pannello di controllo evidenzia i controlli utilizzati nelle valutazioni che presentano prove di verifica della conformità con una conclusione non conforme. Le prove di verifica della conformità si riferiscono ai controlli che utilizzano AWS Config o AWS Security Hub come tipo di fonte di dati. Per questo tipo di prova, Gestione audit riporta il risultato di un controllo di conformità direttamente da tali servizi. Se Security Hub riporta un risultato con esito negativo o se AWS Config riporta un risultato non conforme, Gestione audit classifica le prove come non conformi.

Prove inconcludenti

Le prove sono inconcludenti se un controllo di conformità non è disponibile o applicabile. Di conseguenza, non è possibile effettuare alcuna valutazione di conformità. Questo è il caso se un controllo utilizza AWS Config o AWS Security Hub come tipo di origine dati ma non hai abilitato tali servizi. Questo vale anche se il controllo utilizza un tipo di origine dati che non supporta i controlli di conformità, come prove manuali, chiamate AWS API o AWS CloudTrail.

Se le prove hanno uno stato di controllo di conformità pari a non applicabile nella console, vengono classificate come inconcludenti nel pannello di controllo.

Prove conformi

Le prove sono conformi se da un controllo di conformità non sono stati rilevati problemi. Questo è il caso se Security Hub riporta un risultato Pass o AWS Config riporta un risultato conforme.

Domini di controllo

Il pannello di controllo introduce il concetto di dominio di controllo. Puoi pensare a un dominio di controllo come a una categoria generale di controlli che non è specifica di alcun framework. I raggruppamenti di domini di controllo sono una delle funzionalità più potenti del pannello di controllo. Gestione audit evidenzia i controlli che nelle valutazioni presentano prove non conformi e li raggruppa per dominio di controllo. L'utilizzo di questa funzionalità consente di concentrare gli sforzi di correzione su domini tematici specifici mentre ci si prepara per un audit.

> **Note**
>
> Un dominio di controllo è diverso da un set di controlli. Un set di controlli è un raggruppamento di controlli specifico del framework, in genere definito da un organismo di regolamentazione. Ad esempio, il framework PCI DSS dispone di un set di controllo denominato Requisito 8: identificazione e autenticazione dell'accesso ai componenti del sistema. Questo set di controllo rientra nel dominio di controllo della gestione delle identità e degli accessi.

Eventuale coerenza dei dati

I dati del pannello di controllo alla fine sono coerenti. Ciò significa che, quando si leggono i dati dal pannello di controllo, questi potrebbero non riflettere immediatamente i risultati di un'operazione di scrittura o aggiornamento completata di recente. Se ricontrolli entro qualche ora, la dashboard dovrebbe riportare i dati più recenti.

Dati provenienti da valutazioni eliminate e inattive

La dashboard mostra i dati delle valutazioni attive. Se elimini una valutazione o ne modifichi lo stato in inattiva lo stesso giorno in cui visualizzi il pannello di controllo, i dati per quella valutazione vengono inclusi come segue.

- Valutazioni inattive: se Gestione audit ha raccolto prove per la valutazione prima di modificarla in inattiva, i dati relativi alle prove vengono inclusi nel pannello di controllo e contano per quel giorno.
- Valutazioni inattive: se Gestione audit ha raccolto prove per la valutazione prima di modificarla in inattiva, i dati relativi alle prove vengono inclusi nel pannello di controllo e contano per quel giorno.

Elementi del pannello di controllo

Le seguenti sezioni trattano i diversi componenti del pannello di controllo.

Argomenti

Filtro di valutazione

Puoi utilizzare il filtro di valutazione per concentrarti su una valutazione attiva specifica.

Per impostazione predefinita, la dashboard mostra i dati aggregati per tutte le valutazioni attive. Se desideri visualizzare i dati per una valutazione specifica, applica un filtro di valutazione. Si tratta di un filtro a livello di pagina che si applica a tutti i widget del pannello di controllo.

Per applicare il filtro di valutazione, seleziona una valutazione dall'elenco a discesa nella parte superiore del pannello di controllo. Questo elenco mostra fino a 10 delle tue valutazioni attive. Le valutazioni create più di recente vengono visualizzate per prime. Se hai molte valutazioni attive, puoi iniziare a digitare il nome di una valutazione per trovarla rapidamente. Dopo aver selezionato una valutazione, il pannello di controllo mostra solo i dati relativi a quella valutazione.

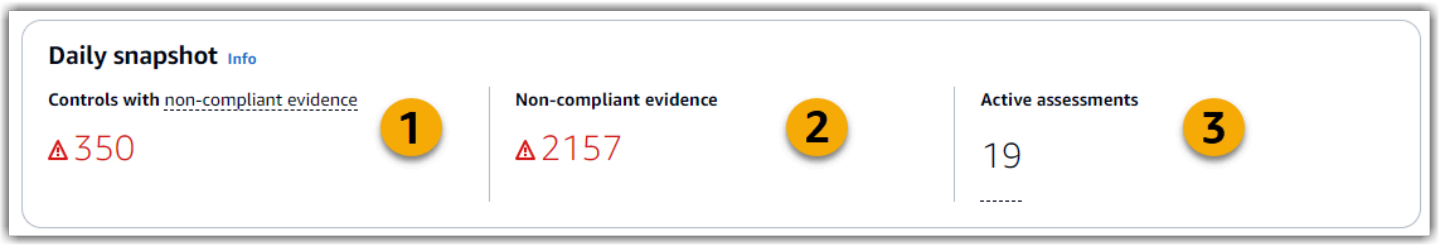
Snapshot giornaliero

Questo widget mostra un'istantanea dello stato di conformità attuale delle valutazioni attive.

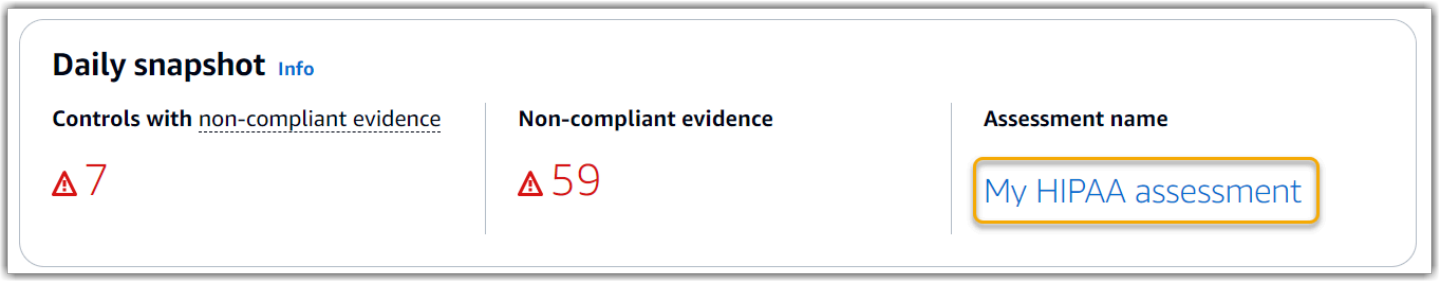
L'istantanea giornaliera riflette i dati più recenti raccolti nella data riportata nella parte superiore del pannello di controllo. La data e l'ora sulla dashboard sono rappresentate in formato UTC. È importante comprendere che questi numeri sono conteggi giornalieri basati su questo timestamp. Ad oggi non sono una somma totale.

Per impostazione predefinita, lo snapshot giornaliero mostra i seguenti dati per tutte le valutazioni attive:

1. Controlli con prove non conformi: il numero totale di controlli associati a prove non conformi.
2. Prove di non conformità: la quantità totale di prove di verifica della conformità con una conclusione non conforme.
3. Valutazioni attive: il numero totale delle valutazioni attive. Scegli questo numero per visualizzare i link a queste valutazioni.



I dati delle istantanee giornaliere cambiano in base a the section called "Filtro di valutazione" quelli applicati. Quando si specifica una valutazione, i dati riflettono i conteggi giornalieri solo per quella valutazione. In questo caso, l'istantanea giornaliera mostra il nome della valutazione specificata. Puoi selezionare il nome della valutazione per aprirla.

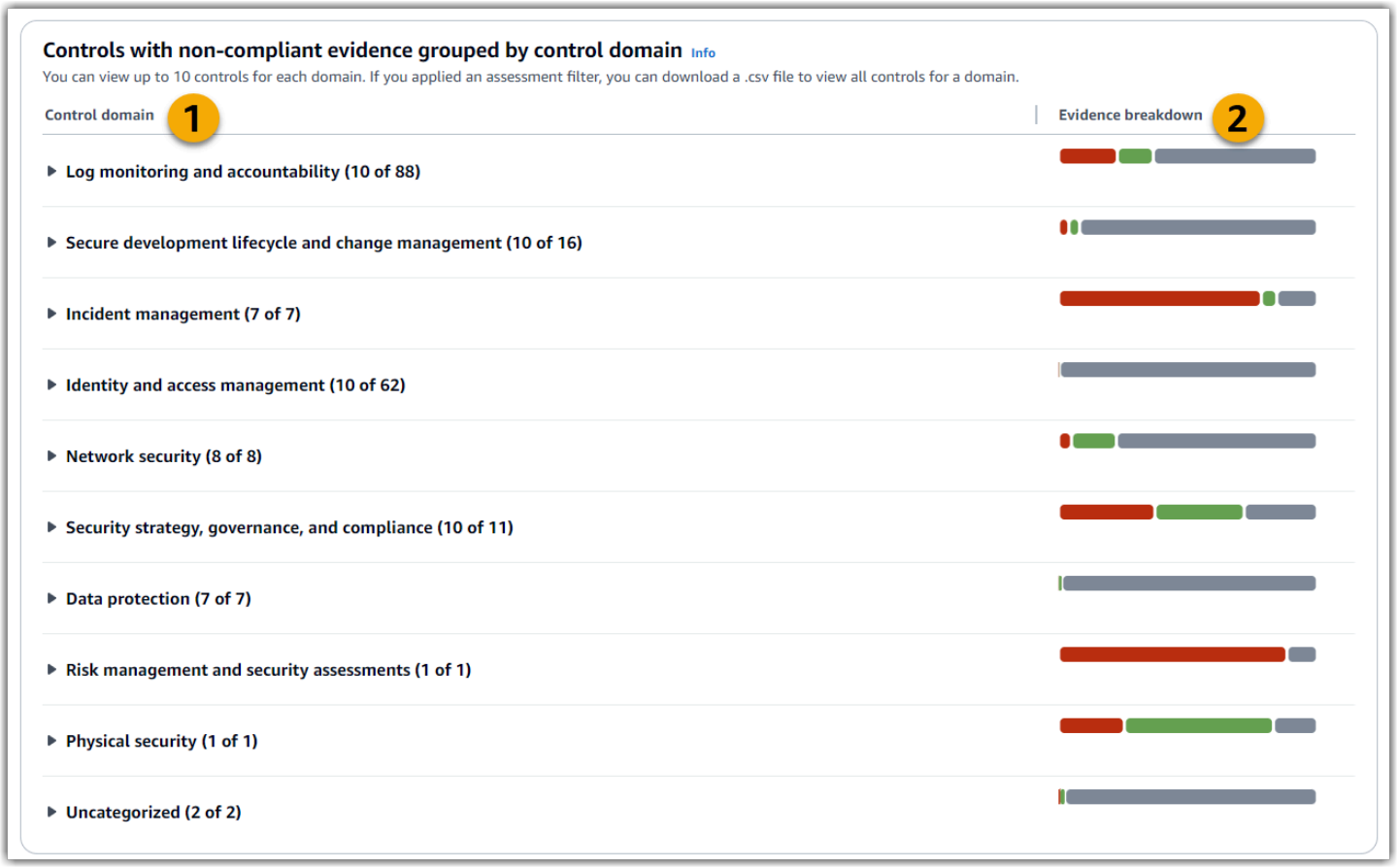


Controlli con prove non conformi raggruppati per dominio di controllo

Puoi utilizzare questo widget per identificare quali controlli presentano le prove più non conformi.

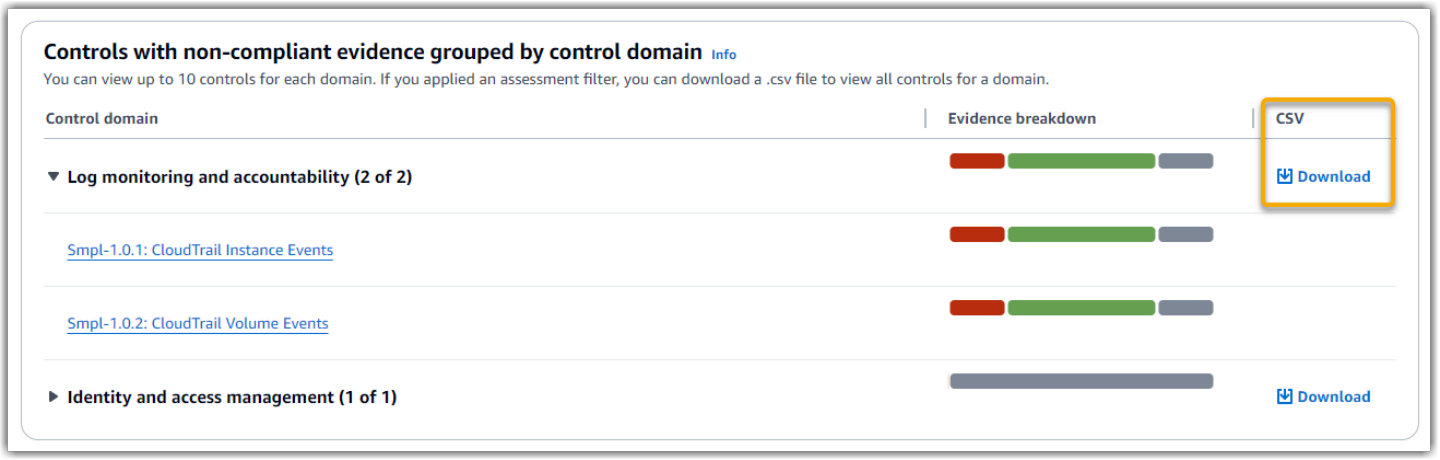
Per impostazione predefinita, il widget mostra i seguenti dati per tutte le valutazioni attive:

1. Dominio di controllo: un elenco di control domains associati alle valutazioni attive.
2. Scomposizione delle prove: un grafico a barre che mostra una suddivisione dello stato di conformità delle prove.



Per espandere un dominio di controllo, scegli la freccia accanto al suo nome. Una volta espansa, la console mostra fino a 10 controlli per ogni dominio. Questi controlli sono classificati in base al numero totale più elevato di prove di non conformità.

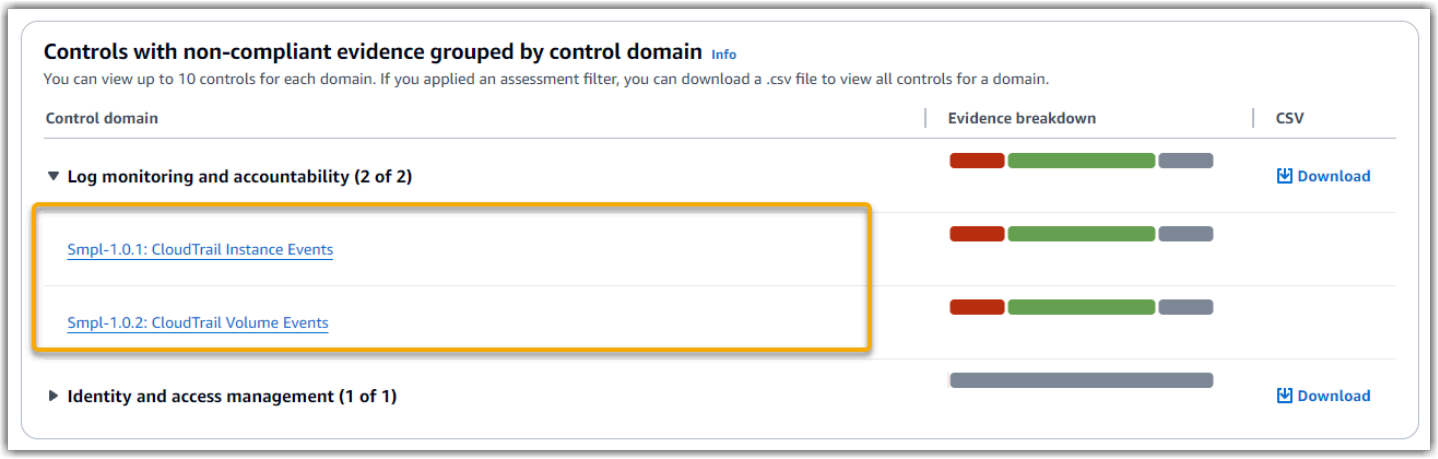
I dati in questo widget cambiano in base ai the section called "Filtro di valutazione" che applichi. Quando si specifica una valutazione, vengono visualizzati solo i dati relativi a quella valutazione. Inoltre, puoi anche scaricare un file CSV per ogni dominio di controllo disponibile nella valutazione.



Il file.csv include l'elenco completo dei controlli del dominio associati a prove di non conformità. L'esempio seguente mostra le colonne di dati CSV con valori fittizi.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Infine, quando si applica un filtro di valutazione, i nomi di controllo di ciascun dominio sono collegati tramite collegamenti ipertestuali. Scegli un controllo qualsiasi per aprire la pagina dei dettagli di controllo nella valutazione specificata.



Tip

Utilizzando la pagina dei dettagli di controllo come punto di partenza, puoi passare da un livello di dettaglio all'altro.

1. Pagina dei dettagli del controllo: in questa pagina, Scheda Cartelle delle prove elenca le cartelle giornaliere di prove raccolte da Audit Manager per quel controllo. Per maggiori dettagli, scegli una cartella.
2. Cartella delle prove: successivamente, è possibile esaminare una cartella Sintesi della cartella Prove e un elenco delle prove contenute in tale cartella. Per maggiori dettagli, scegli un singolo elemento di prova.

3. Prove individuali - Infine, puoi esplorare i dettagli delle singole prove. Questo è il livello più granulare di dati probatori.

Passaggi successivi

Ecco alcuni passaggi successivi che puoi eseguire dopo aver esaminato il pannello di controllo.

- Scarica un file CSV: trova il dominio di valutazione e controllo su cui vuoi concentrarti e scarica l'elenco completo dei controlli correlati con prove non conformi.
- Esamina un controllo: dopo aver identificato un controllo da correggere, puoi esaminare il controllo stesso.
- Delega un controllo per la revisione: se hai bisogno di assistenza per la revisione di un controllo, puoi delegare un set di controlli per la revisione.
- Modifica la valutazione: se desideri modificare l'ambito di una valutazione attiva, puoi modificare la valutazione.
- Aggiorna lo stato della valutazione: se desideri interrompere la raccolta di prove per una valutazione, puoi modificare lo stato della valutazione in inattivo.

Risorse aggiuntive

Per trovare risposte a domande e problemi comuni, consulta la Risoluzione dei problemi della dashboard sezione Risoluzione dei problemi di questa guida.

Gestione delle valutazioni in AWS Audit Manager

Una valutazione Gestione audit si basa su un framework, che è un raggruppamento di controlli. Utilizzando un framework come punto di partenza, è possibile creare una valutazione che raccolga prove dei controlli in quel framework. Nella valutazione, puoi anche definire l'ambito dell'audit. Ciò include la specificazione delle prove per Account AWS cui si desidera raccogliere prove.

Punti chiave

È possibile creare una valutazione da qualsiasi framework. In entrambi i casi, è possibile utilizzare un framework standard fornito da Audit Manager. In alternativa, puoi creare una valutazione da un framework personalizzato creato da te. I framework standard contengono set di controlli predefiniti che supportano uno standard o una normativa di conformità specifici. Al contrario, i framework personalizzati contengono controlli che è possibile personalizzare e raggruppare in base alle proprie esigenze.

La creazione di una valutazione avvia la raccolta continua di prove. Quando è il momento di effettuare un audit, tu o un delegato potete esaminare queste prove e aggiungerle a un rapporto di valutazione.

> **Note**
>
> AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e regolamenti di conformità. Tuttavia, non viene eseguita la valutazione della conformità. AWS Audit Manager Pertanto, le prove raccolte potrebbero non includere tutte le informazioni sull' AWS utilizzo necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Risorse aggiuntive

Per creare e gestire le valutazioni in Audit Manager, segui le procedure descritte qui.

- Creazione di una valutazione in AWS Audit Manager
- Trova le tue valutazioni in AWS Audit Manager
- Revisione di una valutazione in AWS Audit Manager

Creazione di una valutazione in AWS Audit Manager

Questo argomento si basa su. Tutorial per i proprietari degli audit: creazione di una valutazione
In questa pagina troverai istruzioni dettagliate che mostrano come creare una valutazione da un framework. Segui questi passaggi per creare una valutazione e avviare la raccolta continua di prove.

Prerequisiti

Prima di iniziare questo tutorial, assicurati di soddisfare le seguenti condizioni:

- Hai completato tutti i prerequisiti descritti in Configurazione AWS Audit Manager con le impostazioni consigliate. È necessario utilizzare la propria console Account AWS e quella di Audit Manager per completare questo tutorial.
- La tua identità IAM dispone delle autorizzazioni appropriate per creare e gestire una valutazione in Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Attività

- Fase 1: specificare i dettagli della valutazione
- Fase 2: Specificare Account AWS l'ambito
- Fase 3: Specificare i titolari dell'audit
- Fase 4: Revisione e creazione

Fase 1: specificare i dettagli della valutazione

Inizia selezionando un framework e fornendo le informazioni di base per la valutazione.

Specificare i dettagli della valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione selezionare Valutazioni, quindi scegli Crea valutazione.
3. In Nome, inserisci un nome per la valutazione.
4. (Facoltativo) In Descrizione, inserisci una descrizione per la valutazione.
5. In Destinazione dei report di valutazione, seleziona il bucket S3 in cui desideri salvare i report di valutazione.

> **Tip**
>
> La destinazione predefinita del rapporto di valutazione si basa sulle impostazioni di valutazione. Se preferisci, puoi creare e utilizzare più bucket S3 per aiutarti a organizzare i report di valutazione per diverse valutazioni.

6. In Select framework, seleziona il framework da cui vuoi creare la tua valutazione. È anche possibile utilizzare la barra di ricerca per cercare un framework per nome, o per standard di conformità o regolamento.

> **Tip**
>
> Per saperne di più su un framework, scegli il nome del framework per visualizzare la pagina dei dettagli del framework.

7. (Facoltativo) In Tag, scegli Aggiungi nuovo tag per associare un tag alla tua valutazione. Per ogni tag è possibile specificare una chiave e un valore. La chiave di tag è obbligatoria e può essere utilizzata come criterio di ricerca quando cerchi questa valutazione.
8. Seleziona Successivo.

> **Note**
>
> È importante assicurarsi che la valutazione raccolga le prove corrette per un determinato framework. Prima di iniziare la raccolta delle prove, ti consigliamo di esaminare i requisiti del framework prescelto. Quindi, convalida questi requisiti in base ai parametri delle AWS Config regole correnti. Per garantire che i parametri della regola siano in linea con i requisiti del framework, puoi aggiornare la regola in AWS Config.
> Ad esempio, supponiamo che tu stia creando una valutazione per CIS v1.2.0. Questo framework ha un controllo denominato 1.9. Assicurarsi che i criteri delle password IAM richiedano una lunghezza minima di 14 o superiore. In AWS Config, la iam-password-policyregola ha un `MinimumPasswordLength` parametro che controlla la lunghezza della password. Il valore predefinito per questo parametro è 14 caratteri. Di conseguenza, la regola è conforme ai requisiti di controllo. Se non utilizzi il valore del parametro predefinito, assicurati che il valore che stai utilizzando sia uguale o superiore ai 14 caratteri richiesti dal CIS v1.2.0. Puoi trovare i dettagli dei parametri predefiniti per ogni regola gestita nella documentazione AWS Config.

Fase 2: Specificare Account AWS l'ambito

È possibile Account AWS specificarne più di uno da includere nell'ambito di una valutazione. Gestione audit supporta più account tramite l'integrazione con AWS Organizations. Ciò significa che le valutazioni di Audit Manager possono essere eseguite su più account e le prove raccolte vengono

consolidate in un account amministratore delegato. Per abilitare Organizations in Gestione audit, vedere Abilita e configura AWS Organizations (opzionale).

> **Note**
>
> Audit Manager può supportare fino a 200 account nell'ambito di una valutazione. Se si tenta di includere più di 200 account, la creazione della valutazione potrebbe non riuscire.

Da specificare Account AWS nell'ambito

1. In Account AWS, seleziona Account AWS quello che desideri includere nell'ambito della valutazione.
   - Se hai abilitato Organizations in Gestione audit, vengono elencati più account. È possibile scegliere uno o più account dall'elenco. In alternativa, puoi anche cercare un account in base al nome dell'account, all'ID o all'e-mail.
   - Se non hai abilitato Organizations in Audit Manager, Account AWS viene elencata solo la versione corrente.
2. Seleziona Successivo.

> **Note**
>
> Quando un account pertinente viene rimosso dall'organizzazione, Gestione audit non raccoglie più prove per quell'account. Tuttavia, l'account continua a comparire nella valutazione sotto la scheda Account AWS. Per rimuovere l'account dall'elenco degli account in ambito, modifica la valutazione. L'account rimosso non viene più visualizzato nell'elenco durante la modifica ed è possibile salvare le modifiche senza includere tale account nell'ambito.

Fase 3: Specificare i titolari dell'audit

In questa fase, specifica i proprietari dell'audit per la valutazione. I responsabili dell'audit sono le persone sul posto di lavoro, in genere appartenenti a GRC o ai DevOps team SecOps, responsabili della gestione della valutazione dell'Audit Manager. Consigliamo loro di utilizzare la politica. AWSAuditManagerAdministratorAccess

Specificare i proprietari dell'audit

1. Nella sezione Proprietari dell'audit, esamina l'elenco corrente dei titolari dell'audit. La colonna Titolare dell'audit mostra gli ID utente e i ruoli. La Account AWScolonna mostra il titolare Account AWS dell'audit.
2. I proprietari dell'audit che hanno una casella di controllo selezionata sono inclusi nella valutazione. Deselezionare la casella di controllo di un proprietario di audit per rimuoverlo dalla valutazione. Per trovare altri proprietari dell'audit, utilizza la barra di ricerca per nome o Account AWS.
3. Quando hai terminato, seleziona Successivo.

Fase 4: Revisione e creazione

Rivedi le informazioni per la valutazione. Per modificare le informazioni relative a una fase, scegli Modifica. Al termine, scegli Crea valutazione.

La creazione di una valutazione avvia la raccolta continua di prove. Dopo aver creato una valutazione, la raccolta delle prove continua finché non modifichi lo stato della valutazione, impostandolo su inattivo. In alternativa, è possibile interrompere la raccolta delle prove per un controllo specifico modificando lo stato del controllo in inattivo.

> **Note**
>
> Le prove automatizzate diventano disponibili 24 ore dopo la creazione della valutazione. Gestione audit raccoglie automaticamente le prove da più origini dati e la frequenza di tale raccolta di prove si basa sul tipo di evidenza. Per ulteriori informazioni, consulta la Frequenza di raccolta delle prove presente guida.

Passaggi successivi

Per rivedere la valutazione in un secondo momento, vediTrova le tue valutazioni in AWS Audit Manager. Puoi seguire questi passaggi per individuare la tua valutazione in modo da poterla visualizzare, modificare o continuare a lavorarci.

Risorse aggiuntive

Per le soluzioni ai problemi di valutazione in Audit Manager, vedereRisoluzione dei problemi di valutazione e raccolta di prove.

Trova le tue valutazioni in AWS Audit Manager

Dopo aver creato le valutazioni in AWS Audit Manager, puoi trovarle nella pagina delle valutazioni della console Audit Manager.

Da questa pagina, puoi eseguire varie azioni sulle tue valutazioni. Ad esempio, è possibile visualizzare i dettagli della valutazione, modificare le configurazioni della valutazione o eliminare le valutazioni che non sono più necessarie. Inoltre, la pagina delle valutazioni funge da punto di partenza per la creazione di nuove valutazioni.

Puoi anche visualizzare le tue valutazioni in modo programmatico utilizzando l'API Audit Manager o (). AWS Command Line Interface AWS CLI

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione. Se non hai ancora creato una valutazione, non vedrai alcun risultato seguendo questi passaggi.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Puoi visualizzare le tue valutazioni utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare le valutazioni sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.

2. Nel riquadro di navigazione a sinistra, scegli Valutazioni per visualizzare un elenco delle tue valutazioni.
3. Scegli un nome per la valutazione per visualizzarne i dettagli.

AWS CLI

Per visualizzare le tue valutazioni (CLI)

Per visualizzare le valutazioni in Gestione audit, esegui il comando list-assessments. È possibile utilizzare il sottocomando `--status` per visualizzare le valutazioni attive o inattive.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Per visualizzare le tue valutazioni utilizzando l'API

Per visualizzare le valutazioni in Audit Manager, utilizzare l'ListAssessmentsoperazione. È possibile utilizzare l'attributo status per visualizzare le valutazioni attive o inattive.

Per ulteriori informazioni, scegli uno dei link precedenti per saperne di più nel Riferimento API AWS Audit Manager . Ciò include informazioni su come utilizzare l'operazione `ListAssessments` e i parametri in uno degli SDK AWS specifici della lingua.

Passaggi successivi

Quando sei pronto per esplorare i contenuti della valutazione, segui i passaggi indicatiRevisione di una valutazione in AWS Audit Manager. Questa pagina ti guiderà attraverso i dettagli della valutazione e spiegherà le informazioni in essa contenute.

Dalla pagina delle valutazioni, puoi anche modificare una valutazione, eliminare una valutazione o creare una valutazione.

Risorse aggiuntive

Per le soluzioni ai problemi di valutazione in Audit Manager, vedereRisoluzione dei problemi di valutazione e raccolta di prove.

Revisione di una valutazione in AWS Audit Manager

Dopo aver creato le valutazioni in Gestine audit, puoi aprirle e rivederle in qualsiasi momento.

Punti chiave

Quando sei pronto per esplorare la tua valutazione, puoi approfondire gradualmente i dettagli e rivederla con livelli di granularità crescenti.

1. Dettagli della valutazione: inizia esaminando i dettagli generali della valutazione. In questa pagina puoi esaminare il nome, la descrizione, l'ambito e altri dettagli della valutazione. Questo ti offre una panoramica di alto livello della valutazione.
2. Dettagli sul controllo della valutazione: quindi, approfondisci la valutazione esaminando i dettagli di ciascun controllo di valutazione. Ciò ti consentirà di comprendere i requisiti e gli obiettivi specifici di ciascun controllo.
3. Dettagli della cartella delle prove: per ogni controllo di valutazione, è possibile consultare le cartelle delle prove corrispondenti che contengono le prove relative a un determinato controllo. Queste cartelle organizzano le prove di supporto relative a ciascun controllo.
4. Dettagli sulle prove: infine, approfondisci ulteriormente per esaminare le singole prove all'interno di ciascuna cartella. Ciò potrebbe includere istantanee di configurazione, registri delle attività degli utenti, risultati di conformità o prove caricate manualmente come documenti e schermate. La revisione di queste prove ti aiuterà a capire in che modo la tua organizzazione soddisfa i requisiti del controllo.

Seguendo questi passaggi, è possibile esaminare a fondo la valutazione, comprenderne i componenti ed esaminare le prove a sostegno degli sforzi di conformità dell'organizzazione.

Risorse aggiuntive

Per iniziare a esaminare una valutazione in Audit Manager, segui le procedure descritte qui.

- Revisione dei dettagli della valutazione in AWS Audit Manager
- Revisione di un controllo di valutazione in AWS Audit Manager
- Revisione di una cartella di prove in AWS Audit Manager
- Revisione delle prove in AWS Audit Manager

Revisione dei dettagli della valutazione in AWS Audit Manager

Quando hai bisogno di esaminare i dettagli di una valutazione, troverai le informazioni organizzate in diverse sezioni nella pagina dei dettagli della valutazione. Queste sezioni ti aiutano ad accedere e comprendere facilmente le informazioni pertinenti per la tua attività.

Indice

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione. Se non hai ancora creato una valutazione, non vedrai alcun risultato seguendo questi passaggi.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per aprire e rivedere una pagina dei dettagli di una valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Valutazioni per visualizzare un elenco delle tue valutazioni.
3. Scegli il nome della valutazione per aprirla.
4. Rivedi i dettagli della valutazione utilizzando le seguenti informazioni come riferimento.

Sezioni della pagina dei dettagli della valutazione

- Sezione dei dettagli della valutazione
- Scheda Controlli
- Scheda di selezione del report di valutazione
- Account AWS scheda
- Servizi AWS scheda
- Scheda titolari audit
- Scheda Tag
- Scheda Changelog

Sezione dei dettagli della valutazione

Puoi utilizzare la sezione Dettagli della valutazione per visualizzare un riepilogo della valutazione.

Nella sezione dei dettagli della valutazione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
1. Descrizione	La descrizione della valutazione.
2. Tipo di conformità	Lo standard o il regolamento di conformità supportato dalla valutazione.
3. Destinazione dei rapporti di valutazione	Il bucket S3 in cui Audit Manager salva il rapporto di valutazione.
4. Evidenza totale	Il numero totale di elementi di prova raccolti per questa valutazione.
5. Selezione del rapporto di valutazione	Il numero di elementi probatori selezionati per essere inclusi nel rapporto di valutazione.
6. Date created (Data di creazione)	La data in cui è stata creata la valutazione.
7. Ultimo aggiornamento	La data in cui la valutazione è stata modificata l'ultima volta.
8. Stato	Lo stato della valutazione. • Attiva: la valutazione sta attualmente raccogliendo prove. • Inattivo: la valutazione non raccoglie più prove.

Scheda Controlli

È possibile utilizzare questa scheda per visualizzare le informazioni sui controlli della valutazione.

In Riepilogo dello stato del controllo, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Controlli totali	Il numero totale di controlli inclusi in questa valutazione.
Revisionato	Il numero di controlli che sono stati esaminati da un titolare o da un delegato dell'audit.
In fase di revisione	Il numero di controlli attualmente in fase di revisione.

Nome	Descrizione
Inattivo	Il numero di controlli che non raccolgono più prove attivamente

Nella tabella Set di controlli, è possibile esaminare un elenco di controlli raggruppati per set di controlli. È possibile espandere o comprimere i controlli in ogni set di controlli. Puoi anche cercare per nome se stai cercando un controllo specifico.

In questa tabella, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Controlli raggruppati per set di controlli	Il nome del set di controlli.
Stato del controllo	Lo stato del controllo. • In fase di revisione indica che questo controllo non è già stato esaminato. Le prove per questo controllo sono ancora in fase di raccolta ed è possibile aggiungere prove manuali. Questo è lo stato predefinito. • Revisionato indica che le prove relative a questo controllo sono state esaminate. Le prove sono ancora in fase di raccolta ed è possibile aggiungere prove manuali. • Inattivo indica che la raccolta automatica delle prove è stata interrotta per questo controllo. Non è più possibile aggiungere prove manuali.
Delegato a	Il revisore di questo controllo, se è stato assegnato a un delegato per la revisione.
Evidenza totale	Il numero di elementi di prova raccolti per questo controllo.

Scheda di selezione del report di valutazione

È possibile utilizzare questa scheda per visualizzare le prove che verranno incluse nel rapporto di valutazione. Le prove sono raggruppate in cartelle di prove, organizzate in base alla data in cui sono state create.

Puoi sfogliare queste cartelle e selezionare le prove che desideri includere nel report di valutazione. Per istruzioni su come aggiungere prove a un rapporto di valutazione, vedereAggiungere prove a un report di valutazione.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Cartella delle prove	Il nome della cartella delle prove. La cartella viene nominata in base alla data di raccolta delle prove.
Prove selezionate	Il numero di elementi probatori all'interno della cartella inclusi nel rapporto di valutazione.
Nome del controllo	Il nome del controllo associato a questa cartella delle prove.

Account AWS scheda

Puoi usare questa scheda per vedere quelli Account AWS che rientrano nell'ambito della valutazione.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
ID account	L'ID del Account AWS.
Account name (Nome account)	Nome della Account AWS.
E-mail	L'indirizzo e-mail associato all' Account AWS.

Servizi AWS scheda

Potresti vedere o meno questa scheda nella tua valutazione.

Se la Servizi AWS scheda non è visualizzata (stato ideale)

Se non vedi questa scheda, significa che Audit Manager sta gestendo quali Servizi AWS rientrano nell'ambito della tua valutazione.

Audit Manager deduce questo ambito esaminando i controlli di valutazione e le relative fonti di dati e quindi mappando queste informazioni con le corrispondenti. Servizi AWS Ogni volta che una fonte di dati sottostante cambia per la valutazione, Audit Manager aggiorna automaticamente l'ambito secondo necessità per riflettere quello corretto Servizi AWS. Ciò garantisce che la valutazione raccolga prove accurate e complete su tutti i servizi pertinenti presenti nell' AWS ambiente.

Se è Servizi AWS visualizzata la scheda

In tal caso, viene visualizzata questa scheda, significa che Audit Manager non è in grado di gestire Servizi AWS gli elementi che rientrano nell'ambito della valutazione.

In questo caso, vengono visualizzate le seguenti informazioni sui servizi che rientrano nell'ambito definito:

Nome	Descrizione
Servizio AWS	Nome della Servizio AWS.
Categoria	La categoria di servizi, ad esempio elaborazione o database.
Descrizione	La descrizione del Servizio AWS.

Gestione audit esegue valutazioni delle risorse per i servizi in questa tabella. Ad esempio, se Amazon S3 è presente nell'elenco, Gestione audit può raccogliere prove sui bucket S3. Le prove esatte raccolte sono determinate da un controllo. data source Ad esempio, se il tipo di origine dati è AWS Config e la mappatura dell'origine dati è una AWS Config regola (ad esempio`s3-bucket-public-write-prohibited`), Audit Manager raccoglie il risultato della valutazione di tale regola come prova. Per ulteriori informazioni sul tagging, consulta Qual è la differenza tra un servizio in ambito e un tipo di origine dati?in questa guida.

Se la valutazione è stata creata nella console da un framework standard, Gestione audit ha selezionato i servizi per te e ha mappato le loro origini dati in base ai requisiti del framework. Se il framework standard contiene solo controlli manuali, non rientra nell'ambito di Servizi AWS applicazione.

> **Note**
>
> La prossima volta che modificherai la valutazione o cambierai uno dei controlli personalizzati della valutazione, Audit Manager si occuperà della gestione dei servizi previsti per te. Quando ciò accade, la Servizi AWSscheda viene rimossa dalla valutazione.

Scheda titolari audit

È possibile utilizzare questa scheda per visualizzare i proprietari dell'audit per la valutazione.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Proprietario dell'audit	Il nome del titolare dell'audit.
Account AWS	L' Account AWS ID del proprietario dell'audit.

Scheda Tag

Puoi utilizzare questa scheda per visualizzare i tag della tua valutazione. Questi tag vengono ereditati dal framework utilizzato per creare la valutazione. Per ulteriori informazioni sull'utilizzo dei tag in Gestione audit, consulta Taggare le risorse AWS Audit Manager.

In questa sezione, è possibile esaminare le seguenti informazioni:

Nome	Descrizione
Chiave	La chiave del tag, ad esempio uno standard di conformità, un regolamento o una categoria.
Valore	Il valore del tag.

Scheda Changelog

Puoi utilizzare questa scheda per visualizzare l'attività dell'utente per la valutazione.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Data	La data dell'attività.
Utente	L'utente che ha eseguito l'azione.
Action	L'azione che si è verificata, ad esempio la creazione di una valutazione.
Type	Il tipo di oggetto modificato, ad esempio una valutazione.
Resource (Risorsa)	La risorsa interessata dalla modifica, ad esempio il framework da cui è stata creata la valutazione.

Passaggi successivi

Per continuare a esaminare i contenuti della valutazione, segui la procedura riportata di seguitoRevisione di un controllo di valutazione in AWS Audit Manager. Questa pagina ti guiderà attraverso i dettagli della valutazione e del controllo e spiegherà le informazioni in essa contenute.

Risorse aggiuntive

- Nella pagina dei dettagli della mia valutazione, mi viene richiesto di ricreare la mia valutazione
- Non riesco a vedere alcun controllo o set di controlli nella mia valutazione
- Non riesco a visualizzare i servizi oggetto della mia valutazione

Revisione di un controllo di valutazione in AWS Audit Manager

Quando devi rivedere i controlli di una valutazione, troverai le informazioni organizzate in diverse sezioni nella pagina dei dettagli del controllo di valutazione. Queste sezioni ti aiutano ad accedere e comprendere facilmente le informazioni pertinenti per la tua attività.

Indice

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione. Se non hai ancora creato una valutazione, non vedrai alcun risultato seguendo questi passaggi.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per aprire e rivedere una pagina dei dettagli di valutazione e controllo

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Valutazioni e scegli il nome di una valutazione per aprirla.
3. Per la pagina di valutazione, scegli la scheda Controlli, scorri verso il basso fino alla tabella Set di controlli, quindi seleziona il nome di un controllo per aprirlo.
4. Esamina i dettagli del controllo della valutazione utilizzando le seguenti informazioni come riferimento.

Sezioni della pagina dei dettagli del controllo della valutazione

- Sezione relativa ai dettagli del controllo
- Scheda Cartelle delle prove
- Scheda Dettagli
- Scheda Fonti di prova
- Scheda Commenti
- Scheda Changelog

Sezione relativa ai dettagli del controllo

È possibile utilizzare la sezione Dettagli del controllo per visualizzare un riepilogo del controllo di valutazione.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Description
Descrizione	La descrizione fornita per questo controllo.
Stato del controllo	Lo stato del controllo. • In fase di revisione: il controllo non è stato ancora esaminato. Le prove per questo controllo sono ancora in fase di raccolta ed è possibile aggiungere prove manuali. Questo è lo stato predefini to. • Revisionato: le prove relative a questo controllo vengono esaminate. Le prove sono ancora in fase di raccolta ed è possibile aggiungere prove manuali. • Inattivo: la raccolta automatica delle prove viene interrotta per questo controllo. Non è più possibile aggiungere prove manuali.

Scheda Cartelle delle prove

Puoi utilizzare questa scheda per visualizzare le prove raccolte per questo controllo. È organizzata in cartelle su base giornaliera. Da qui, puoi anche eseguire le seguenti azioni:

- Rivedi una cartella di prove: per visualizzare i dettagli di qualsiasi cartella di prove, scegli il nome della cartella con collegamento ipertestuale.

- Aggiungi una cartella di prove a un rapporto di valutazione: per includere una cartella di prove, selezionala e scegli Aggiungi al rapporto di valutazione.
- Rimuovi una cartella di prove da un rapporto di valutazione: per escludere una cartella, selezionala e scegli Rimuovi dal rapporto di valutazione.
- Aggiungi prove manuali: per istruzioni, consultaAggiungere prove manuali in AWS Audit Manager.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Cartella delle prove	Il nome della cartella delle prove. La cartella viene nominata in base alla data di raccolta o aggiunta manuale delle prove.
Controllo della conformità	Il numero di problemi nella cartella delle prove. Questo numero rappresenta il numero totale di problemi di sicurezza segnalati direttamente da AWS Security Hub o da entrambi. AWS Config Se vedi Non applicabile, significa che Security Hub non è AWS Config abilitato o che la prova proviene da un tipo di origine dati diverso.
Evidenza totale	Il numero totale di elementi di prova all'interno della cartella.
Selezione del rapporto di valutazione	Il numero di elementi probatori all'interno della cartella inclusi nel rapporto di valutazione.

> **Tip**
>
> Se non riesci a visualizzare la cartella delle prove che stai cercando, modifica il filtro a discesa su Sempre. Altrimenti, per impostazione predefinita, verranno visualizzate le cartelle degli ultimi sette giorni.

Scheda Dettagli

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Informazioni sui test	Procedura consigliata per verificare che il controllo funzioni come previsto.
Piano d'azione	Le azioni consigliate da intraprendere se è necessario porre rimedio al controllo.

Scheda Fonti di prova

Puoi utilizzare questa scheda per vedere da dove il controllo di valutazione raccoglie le prove. Le fonti di evidenza possono includere uno dei seguenti elementi:

Nome	Descrizione
Controlli comuni	Questi sono i controlli comuni che raccolgono prove a supporto del controllo della valutazione. I controlli comuni raccolgono prove utilizzando fonti di dati sottostanti che AWS gestiscono per te. Per ogni controllo comune elencato, Audit Manager raccoglie le prove pertinenti per tutti i controlli principali di supporto. Scegli un controllo comune per visualizzare i controlli principali correlati.
Controlli principali	Questi sono i controlli principali che raccolgono prove a supporto del controllo della valutazione. I controlli principali raccolgono prove utilizzando un gruppo predefinito di fonti di dati che AWS gestiscono per te. Scegli un controllo di base per visualizzare le fonti di dati sottostanti.
Fonti di dati	Queste sono le singole fonti di dati che raccolgono prove a supporto del controllo della valutazione. • Nome: il nome della fonte di dati. • Tipo: il tipo di fonte di dati da cui provengono le prove.

Nome	Descrizione
	• Se Audit Manager raccoglie le prove, il tipo può essere AWS Security Hub, AWS ConfigAWS CloudTrail, o chiamate AWS API. • Se carichi le tue prove, il tipo è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale. • Mappatura: la parola chiave specifica utilizzata per raccogliere prove. • Se il tipo è AWS Config, la mappatura è una AWS Config regola (ad esempio) `SNS_ENCRYPTED_KMS` • Se il tipo è AWS Security Hub, la mappatura è un controllo del Security Hub (ad esempio`EC2.1`). • Se il tipo è una chiamata AWS API, la mappatura è una chiamata API (ad esempio`kms_ListKeys`). • Se il tipo è AWS CloudTrail, la mappatura è un CloudTrail evento (ad esempio`CreateAccessKey`). • Frequenza: con quale frequenza Audit Manager raccoglie prove per un'origine dati di chiamata AWS API.

Scheda Commenti

In questa scheda, puoi aggiungere un commento sul controllo e sulle relative prove. Puoi anche visualizzare un elenco di commenti precedenti.

- In Invia commenti, è possibile aggiungere commenti per un controllo inserendo il testo e scegliendo Invia commenti.
- In Commenti precedenti, è possibile visualizzare un elenco di commenti precedenti insieme alla data di creazione del commento e all'ID utente associato.

Scheda Changelog

È possibile utilizzare questa scheda per visualizzare l'attività dell'utente per il controllo della valutazione. Le stesse informazioni sono disponibili come log di audit trail. AWS CloudTrail Con

l'attività dell'utente acquisita direttamente in Gestione audit , puoi facilmente esaminare un audit trail delle attività per un determinato controllo.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Data	La data e l'ora dell'attività, rappresentate in UTC (Coordinated Universal Time).
Utente	L'utente o il ruolo che ha eseguito l'attività.
Action	L'azione che si è verificata, ad esempio la creazione di una valutazione.
Type	Il tipo di oggetto modificato, ad esempio una valutazione.
Resource (Risorsa)	La risorsa interessata dalla modifica, ad esempio il framework da cui è stata creata la valutazione.

Gestione audit tiene traccia delle seguenti attività degli utenti nei changelog:

- Creazione di una valutazione
- Modifica di una valutazione
- Completamento di una valutazione
- Eliminazione di una valutazione
- Delega di un set di controllo per la revisione
- Invio di un set di controllo revisionato al titolare dell'audit
- Caricamento di prove manuali
- Aggiornamento dello stato di controllo
- Generazione di report di valutazione

Passaggi successivi

Per continuare a esaminare la valutazione, segui la procedura riportata di seguitoRevisione di una cartella di prove in AWS Audit Manager. Questa pagina ti guiderà attraverso le cartelle delle prove e ti mostrerà come comprendere le informazioni che vedi.

Risorse aggiuntive

- Non riesco a vedere alcun controllo o set di controlli nella mia valutazione

Revisione di una cartella di prove in AWS Audit Manager

Man mano che la valutazione raccoglie le prove, Audit Manager le organizza in cartelle per comodità dell'utente. Quando devi esaminare una cartella delle prove, troverai le informazioni organizzate in diverse sezioni.

Indice

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione. Se non hai ancora creato una valutazione, non vedrai alcun risultato seguendo questi passaggi.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Tieni presente che sono necessarie fino a 24 ore prima che una valutazione inizi a raccogliere prove automatizzate. Se la tua valutazione non contiene ancora prove, non vedrai alcun risultato seguendo questi passaggi.

Procedura

Per aprire e rivedere una cartella delle prove

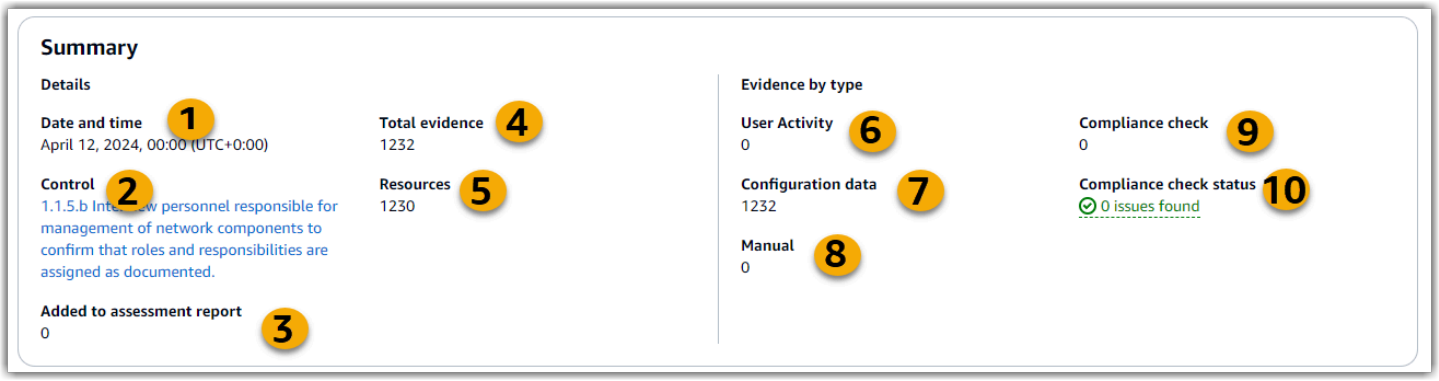
1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Valutazioni, quindi scegli una valutazione.
3. Dalla pagina di valutazione, scegli la scheda Controlli, scorri verso il basso fino alla tabella Controlli, quindi scegli un controllo di valutazione.
4. Dalla pagina di controllo della valutazione, scegli la scheda Cartelle Evidence.
5. Nella tabella delle cartelle delle prove, scegli il nome di una cartella di prove.
6. Esamina la cartella delle prove utilizzando le seguenti informazioni come riferimento.

Sezioni di una pagina della cartella delle prove

- Sintesi della cartella Prove
- Tabella delle prove

Sintesi della cartella Prove

Puoi utilizzare la sezione Riepilogo della pagina per visualizzare una panoramica di alto livello delle prove contenute nella cartella delle prove. Per ulteriori informazioni sui diversi tipi di prove, consulta Evidence.



In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
1. Data e ora	L'ora e la data in cui è stata creata la cartella delle prove. È rappresentata nel Coordinated Universal Time (UTC).
2. Controllo	Il nome del controllo collegato alla cartella delle prove.
3. Aggiunto al rapporto di valutazione	Il numero di elementi probatori selezionati per essere inclusi nel rapporto di valutazione.
4. Evidenza totale	Il numero totale di elementi di prova nella cartella delle prove.
5. Risorse	Il numero totale di AWS risorse che sono state valutate durante la raccolta delle prove in questa cartella.
6. Attività dell'utente	Il numero di elementi di prova che rientrano nella categoria delle attività degli utenti. Queste prove vengono raccolte dai AWS CloudTrail log.
7. Dati di configurazione	Il numero di elementi di prova che rientrano nella categoria dei dati di configurazione. Queste prove vengono raccolte dalle chiamate API che acquisiscono istantanee di configurazione di altri Servizi AWS.
8. Manuale	Il numero di elementi di prova che rientrano nella categoria dei manuali. Queste prove vengono aggiunte manualmente.
9. Controllo della conformità	Il numero di elementi di prova che rientrano nella categoria del controllo di conformità. Queste prove vengono raccolte da AWS Config AWS Security Hub, o da entrambi.
10. Stato del controllo di conformità	Il numero totale di problemi segnalati direttamente da AWS Security Hub o da entrambi. AWS Config

Tabella delle prove

Puoi utilizzare la tabella Evidenze per visualizzare le prove contenute nella cartella delle prove. Da questa tabella, puoi anche eseguire le seguenti azioni:

- Esamina le singole prove: per visualizzare i dettagli di ogni prova, scegli il nome della prova con collegamento ipertestuale nella colonna Ora.
- Aggiungi prove a un rapporto di valutazione: per includere prove, selezionale e scegli Aggiungi al rapporto di valutazione.
- Rimuovi prove da un rapporto di valutazione: per escludere prove, selezionale e scegli Rimuovi dal rapporto di valutazione.
- Aggiungi prove manuali: per istruzioni, vediAggiungere prove manuali in AWS Audit Manager.

In questa tabella, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Time (Orario)	Speciifica quando sono state raccolte le prove. Serve anche come nome della prova. L'ora è presentata in formato UTC (Universal Time Code, codice orario universale).
Controllo della conformità	Lo stato di valutazione delle prove che rientrano nella categoria del controllo di conformità. • Per le prove raccolte da Security Hub, un risultato positivo o negativo viene segnalato direttamente da Security Hub. • Per le prove raccolte da AWS Config, un risultato conforme o non conforme viene segnalato direttamente da. AWS Config • Se viene visualizzato Non applicabile, significa che Security Hub non è abilitato o che l'evidenza proviene da un tipo di origine dati diverso. AWS Config
Prove per tipo	Il tipo di prova. • Le prove relative al controllo di conformità vengono raccolte da AWS Config o AWS Security Hub. • Le prove dell'attività degli utenti vengono raccolte da AWS CloudTrail. • Le prove dei dati di configurazione vengono raccolte dalle chiamate API ad altri Servizi AWS.

Nome	Descrizione
	• Le prove manuali sono prove che vengono aggiunte manualmente.
Origine dati	La fonte di dati da cui vengono raccolte le prove.
Nome evento	Il nome dell'evento che ha richiamato la raccolta delle prove.
Origine eventi	Il responsabile del servizio che identifica il soggetto rilevante Servizio AWS per l'evento.
Risorse	Il numero di risorse che sono state valutate durante la raccolta delle prove.
Selezione del rapporto di valutazione	Indica se le prove sono incluse nel rapporto di valutazione. • Per includere le prove, seleziona le prove e scegli Aggiungi al report di valutazione. • Per escludere le prove, seleziona le prove e scegli Rimuovi dal report di valutazione.

Passaggi successivi

Quando sei pronto per esplorare le singole prove contenute in una cartella, segui i passaggi indicati di seguitoRevisione delle prove in AWS Audit Manager. Questa pagina ti guiderà attraverso i dettagli delle prove e come interpretare le informazioni in esse contenute.

Risorse aggiuntive

- Per le soluzioni ai problemi relativi alle prove in Audit Manager, vedereRisoluzione dei problemi di valutazione e raccolta di prove.

Revisione delle prove in AWS Audit Manager

Quando devi esaminare una prova specifica, segui le istruzioni riportate in questa pagina. Troverai i dettagli delle prove organizzati in diverse sezioni.

Indice

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione. Se non hai ancora creato una valutazione, non vedrai alcun risultato seguendo questi passaggi.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Tieni presente che sono necessarie fino a 24 ore prima che una valutazione inizi a raccogliere prove automatizzate. Se la tua valutazione non contiene ancora prove, non vedrai alcun risultato seguendo questi passaggi.

Procedura

Per aprire e rivedere la pagina dei dettagli delle prove

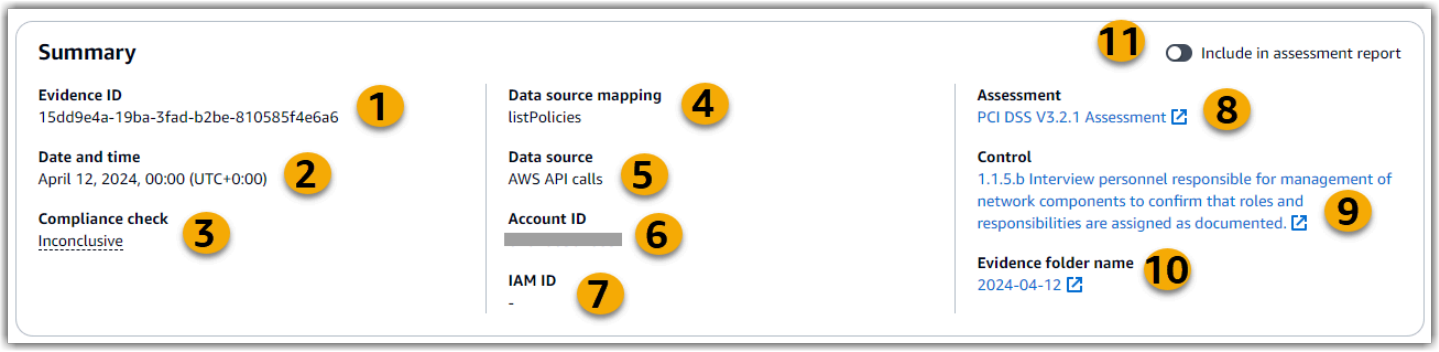
1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Valutazioni, quindi scegli una valutazione.
3. Dalla pagina di valutazione, scegli la scheda Controlli, scorri verso il basso fino alla tabella Controlli, quindi scegli un controllo.
4. Dalla pagina del controllo, scegli la scheda Cartelle di prove.
5. Nella tabella delle cartelle delle prove, scegli il nome di una cartella di prove.
6. Scegli il nome della prova nella colonna Ora per aprire la pagina dei dettagli delle prove.
7. Esamina i dettagli delle prove utilizzando le seguenti informazioni come riferimento.

Sezioni della pagina dei dettagli delle prove

- Riepilogo
- Attributes
- Risorse incluse

Riepilogo

Puoi utilizzare la sezione Riepilogo per visualizzare una panoramica delle prove.



In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
1. ID delle prove	L'identificatore univoco delle prove.
2. Data e ora	L'ora e la data in cui sono state raccolte le prove. Questo è rappresentato nel Coordinated Universal Time (UTC).
3. Controllo della conformità	Lo stato di valutazione degli elementi probatori del controllo di conformità. • Per le prove raccolte da AWS Security Hub, un risultato positivo o negativo viene segnalato direttamente da AWS Security Hub. • Per le prove raccolte da AWS Config, un risultato conforme o non conforme viene segnalato direttamente da. AWS Config • Se viene visualizzato Non applicabile, ciò indica una delle due cose. O non lo hai AWS Security Hub o lo hai AWS Config abilitato. Oppure, le prove provengono da una fonte di dati diversa.

Nome	Descrizione
4. Mappatura delle fonti di dati	La parola chiave di mappatura utilizzata per raccogliere le prove.
5. Data source type (Tipo di origine dati)	Il tipo di fonte di dati da cui sono state raccolte le prove.
6. ID account	Quello Account AWS che è associato alle prove.
7. ID IAM	L'utente o il ruolo pertinente, se applicabile.
8. Valutazione	Il nome della valutazione associata alle prove.
9. Controllo	Il nome del controllo associato alle prove.
10. Nome della cartella delle prove	Il nome della cartella delle prove che contiene le prove.
11. Includi nel rapporto di valutazione	L'interruttore che consente di includere o escludere le prove dal rapporto di valutazione.

Attributes

È possibile utilizzare la tabella Attributi per visualizzare in dettaglio gli attributi delle prove.

In questa tabella, puoi esaminare le seguenti informazioni:

Nome	Descrizione
Nome attributo	La chiave per l'attributo.
Valore	Il valore dell'attributo. In alcuni casi, viene fornito un collegamento a un file JSON con ulteriori informazioni.

Risorse incluse

È possibile utilizzare la tabella Risorse incluse per visualizzare le risorse che sono state valutate per generare queste evidenze.

In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Descrizione
ARN	Il nome della risorsa Amazon (ARN) della risorsa . Un ARN potrebbe non essere disponibile per tutti i tipi di prove.
Conformità delle risorse	Lo stato di valutazione della risorsa. • Per le prove raccolte da AWS Security Hub, un risultato positivo o negativo viene segnalato direttamente da Security Hub. • Per le prove raccolte da AWS Config, un risultato conforme o non conforme viene segnalato direttamente da. AWS Config • Se viene visualizzato Non applicabile, significa che Security Hub non è abilitato o che l'evidenza proviene da un'altra fonte di dati. AWS Config
Valore	Ulteriori informazioni sulla valutazione delle risorse. In alcuni casi, viene fornito un collegamento a un file JSON con ulteriori informazioni.

Risorse aggiuntive

- Per le soluzioni ai problemi relativi alle prove in Audit Manager, vedereRisoluzione dei problemi di valutazione e raccolta di prove.

Modificare una valutazione in AWS Audit Manager

Potresti riscontrare situazioni in cui devi modificare le valutazioni esistenti in AWS Audit Manager. Forse l'ambito dell'audit è cambiato e sono necessari aggiornamenti rispetto a quanto Account AWS incluso nella valutazione. In alternativa, potrebbe essere necessario rivedere l'elenco dei responsabili dell'audit assegnati alla valutazione a causa di cambiamenti di personale. In questi casi, è possibile modificare le valutazioni attive e apportare le modifiche necessarie senza interrompere la raccolta delle prove.

La pagina seguente descrive i passaggi per modificare i dettagli della valutazione, cambiarne l' Account AWS ambito, aggiornare i proprietari dell'audit e rivedere e salvare le modifiche.

Prerequisiti

La procedura seguente presuppone che in precedenza sia stata creata almeno una valutazione e che questa sia attiva.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per modificare una valutazione. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Attività

- Fase 1: modificare i dettagli della valutazione
- Fase 2: Modifica Account AWS l'ambito
- Fase 3: Modifica dei proprietari dell'audit
- Passaggio 4: rivedi e salva

Fase 1: modificare i dettagli della valutazione

Segui questi passaggi per modificare i dettagli della valutazione.

Per modificare una valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Valutazioni.
3. Seleziona una valutazione e scegli Modifica.
4. In Modifica i dettagli della valutazione, modifica i dettagli della valutazione in base alle tue esigenze.
5. Seleziona Successivo.

Fase 2: Modifica Account AWS l'ambito

In questo passaggio, puoi modificare gli account inclusi nella valutazione. Audit Manager può supportare fino a 200 account nell'ambito di una valutazione.

Da modificare Account AWS nell'ambito

1. Per aggiungere un Account AWS, seleziona la casella di controllo accanto al nome dell'account.
2. Per rimuoverne uno Account AWS, deseleziona la casella di controllo accanto al nome dell'account.
3. Seleziona Successivo.

> **Note**
>
> Per modificare l'amministratore delegato per Audit Manager, vedereModifica di un amministratore delegato.

Fase 3: Modifica dei proprietari dell'audit

In questo passaggio, puoi modificare i titolari dell'audit inclusi nella valutazione.

Per modificare i proprietari dell'audit

1. Per aggiungere un titolare dell'audit, seleziona la casella di controllo accanto al nome dell'account.
2. Per rimuovere il proprietario di un audit, deseleziona la casella di controllo accanto al nome dell'account.
3. Seleziona Successivo.

Passaggio 4: rivedi e salva

Rivedi le informazioni per la valutazione. Per modificare le informazioni relative a una fase, scegli Modifica. Al termine della modifica, scegli Salva modifiche per confermare le modifiche.

Dopo aver completato le modifiche, le modifiche alla valutazione entreranno in vigore alle 00:00 UTC del giorno successivo.

Passaggi successivi

Quando non è più necessario raccogliere prove per uno specifico controllo di valutazione, è possibile modificare lo stato di tale controllo. Per istruzioni, consulta Modifica dello stato di un controllo di valutazione in AWS Audit Manager.

Quando non è più necessario raccogliere prove per l'intera valutazione, è possibile modificare lo stato della valutazione in inattivo. Per istruzioni, consulta Modificare lo stato di una valutazione in inattiva in AWS Audit Manager.

Risorse aggiuntive

- Per le soluzioni ai problemi di valutazione in Audit Manager, vedereRisoluzione dei problemi di valutazione e raccolta di prove.
- Per informazioni sul motivo per cui non è più possibile modificare i servizi inclusi nell'ambito, consulta Non riesco a modificare i servizi in ambito per la mia valutazione la sezione Risoluzione dei problemi di questa guida.

Aggiungere prove manuali in AWS Audit Manager

Gestione audit può raccogliere automaticamente prove per molti controlli. Tuttavia, alcuni controlli potrebbero richiedere prove che non possono essere raccolte automaticamente. In questi casi, puoi aggiungere manualmente le tue prove.

Considerare i seguenti esempi:

- Alcuni controlli riguardano la fornitura di record fisici (come le firme) o di eventi che non vengono generati nel cloud (come osservazioni e interviste). In questi casi, puoi aggiungere manualmente i file come prova. Ad esempio, se un controllo richiede informazioni sulla struttura organizzativa, è possibile caricare una copia dell'organigramma aziendale come prova manuale.
- Alcuni controlli rappresentano una domanda di valutazione del rischio del fornitore. Una domanda di valutazione del rischio potrebbe richiedere la documentazione come prova (ad esempio un organigramma). In alternativa, potrebbe essere necessaria solo una semplice risposta testuale (ad esempio un elenco di titoli professionali). In quest'ultimo caso, puoi rispondere alla domanda e salvare la risposta come prova manuale.

Puoi anche utilizzare la funzionalità di caricamento manuale per gestire le prove da più ambienti. Se la tua azienda utilizza un modello di cloud ibrido o un modello multicloud, puoi caricare prove dal tuo ambiente on-premise, da un ambiente ospitato nel cloud o dalle tue applicazioni SaaS. Ciò consente di organizzare le prove (indipendentemente dalla loro provenienza) archiviandole all'interno della struttura di valutazione di un Gestione audit, in cui ogni evidenza è mappata su un controllo specifico.

Punti chiave

Quando si tratta di aggiungere prove manuali alle valutazioni in Audit Manager, sono disponibili tre metodi tra cui scegliere.

1. Importazione di un file da Amazon S3: questo metodo è ideale quando in un bucket S3 sono archiviati file di prove, come documentazione, report o altri elementi che non possono essere raccolti automaticamente da Audit Manager. Importando questi file direttamente da S3, puoi integrare senza problemi queste prove manuali con le prove raccolte automaticamente.
2. Caricamento di un file dal browser: se disponi di file di prove archiviati localmente sul computer o sulla rete, puoi caricarli manualmente su Audit Manager utilizzando questo metodo. Questo approccio è particolarmente utile quando è necessario includere documenti fisici, come documenti o immagini scansionati, che non sono disponibili in formato digitale nel proprio AWS ambiente.
3. Aggiungere testo in formato libero come prova: in alcuni casi, le prove da fornire non sono sotto forma di file ma piuttosto di risposta o spiegazione testuale. Questo metodo consente di inserire testo in formato libero direttamente in Audit Manager. Ciò può essere particolarmente utile quando si risponde a domande sulla valutazione del rischio del fornitore.

Risorse aggiuntive

- Per istruzioni su come aggiungere prove manuali a un controllo di valutazione, consulta le seguenti risorse. Tieni presente che puoi utilizzare solo un metodo alla volta.
  - Importazione di file di prove manuali da Amazon S3
  - Caricamento manuale di file di prove dal browser
  - Inserimento di risposte di testo in formato libero come prova manuale
- Per sapere quali formati di file puoi usare, consultaFormati di file supportati per prove manuali.
- Per ulteriori informazioni sui diversi tipi di prove in Audit Manager, vedere evidence la sezione Concetti e terminologia di questa guida.

- Per assistenza nella risoluzione dei problemi, vedereNon riesco a caricare prove manuali su un controllo.

Importazione di file di prove manuali da Amazon S3

Puoi importare manualmente i file di prove da un bucket Amazon S3 nella tua valutazione. Ciò consente di integrare le prove raccolte automaticamente con materiali di supporto aggiuntivi.

Prerequisiti

- La dimensione massima supportata per un singolo file di prove manuali è 100 MB.
- È necessario utilizzare uno deiFormati di file supportati per prove manuali.
- Ciascuno Account AWS può caricare manualmente fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera causa il fallimento di qualsiasi altro caricamento manuale per quel controllo. Se devi caricare una grande quantità di prove manuali su un unico controllo, caricale in batch nell'arco di diversi giorni.
- Quando un controllo è nello stato inattivo, non puoi aggiungere prove manuali relative a quel controllo. Per aggiungere prove manuali, devi prima modificare lo stato del controllo impostandolo su In revisione o in revisione.
- Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per gestire una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile importare un file utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

Per importare un file da S3 sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Valutazioni, quindi scegli una valutazione.

3. Scegli la scheda Controlli, scorri verso il basso fino a Set di controllo, quindi scegli un controllo.
4. Nella scheda Cartelle di prove, scegli Aggiungi prove manuali, quindi scegli Importa file da S3.
5. Nella pagina successiva, inserisci l'URI S3 delle prove. Puoi trovare l'URI S3 accedendo all'oggetto nella console Amazon S3 e scegliendo Copia URI S3.
6. Scegli Carica.

AWS CLI

Nella procedura seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

Per importare un file da S3 in AWS CLI

1. Esegui il `list-assessments` comando per visualizzare un elenco delle tue valutazioni.

```
aws auditmanager list-assessments
```

   Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Esegui il `get-assessment` comando e specifica l'ID di valutazione sin dal primo passaggio.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Nella risposta, individua il set di controlli e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.
3. Usa il comando `batch-import-evidence-to-assessment-control` con i parametri seguenti:

   - `--assessment-id`: usa l'ID di valutazione della prima fase.
   - `--control-set-id`: usa l'ID del set di controllo del secondo passaggio.
   - `--control-id`: usa l'ID di controllo del secondo passaggio.
   - `--manual-evidence`: usa `s3ResourcePath` come tipo di prova manuale e specifica l'URI S3 della prova. Puoi trovare l'URI S3 accedendo all'oggetto nella console Amazon S3 e scegliendo Copia URI S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
DOC-EXAMPLE-BUCKET/EXAMPLE-FILE.extension
```

Audit Manager API

Per importare un file da S3 utilizzando l'API

1. Chiama l'`ListAssessments` operazione per visualizzare un elenco delle tue valutazioni. Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Esegui l'`GetAssessment` operazione e specifica l'ID di valutazione sin dal primo passaggio. Nella risposta, individua il set di controlli e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.
3. Chiama l'operazione `BatchImportEvidenceToAssessmentControl`con i parametri seguenti:
   - `assessmentId`: usa l'ID di valutazione della prima fase.
   - `controlSetId`: usa l'ID del set di controllo del secondo passaggio.
   - `controlId`: usa l'ID di controllo del secondo passaggio.
   - `manualEvidence`: usa `s3ResourcePath` come tipo di prova manuale e specifica l'URI S3 della prova. Puoi trovare l'URI S3 accedendo all'oggetto nella console Amazon S3 e scegliendo Copia URI S3.

Per ulteriori informazioni, scegli uno dei link nella procedura precedente per saperne di più nell'AWS Audit Manager API Reference. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Dopo aver aggiunto e esaminato le prove per la valutazione, puoi generare un rapporto di valutazione. Per ulteriori informazioni, consulta Preparazione di un rapporto di valutazione in AWS Audit Manager.

Altre risorse

Per sapere quali formati di file puoi usare, consultaFormati di file supportati per prove manuali.

Caricamento manuale di file di prove dal browser

Puoi caricare manualmente i file di prove dal tuo browser nella tua valutazione Audit Manager. Ciò consente di integrare le prove raccolte automaticamente con materiali di supporto aggiuntivi.

Prerequisiti

- La dimensione massima supportata per un singolo file di prove manuali è 100 MB.
- È necessario utilizzare uno deiFormati di file supportati per prove manuali.
- Ciascuno Account AWS può caricare manualmente fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera causa il fallimento di qualsiasi altro caricamento manuale per quel controllo. Se devi caricare una grande quantità di prove manuali su un unico controllo, caricale in batch nell'arco di diversi giorni.
- Quando un controllo è nello stato inattivo, non puoi aggiungere prove manuali relative a quel controllo. Per aggiungere prove manuali, devi prima modificare lo stato del controllo impostandolo su In revisione o in revisione.
- Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per gestire una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile caricare un file utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

Per caricare un file dal browser sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.

2. Nel riquadro di navigazione a sinistra, scegli Valutazioni, quindi scegli una valutazione.
3. Nella scheda Controlli, scorri verso il basso fino a Set di controllo, quindi scegli un controllo.
4. Dalla scheda Cartelle delle prove, scegli Aggiungi prove manuali.
5. Scegli Carica file dal browser.
6. Scegli il file che si desidera caricare.
7. Scegli Carica.

AWS CLI

Nella procedura seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

Per caricare un file dal tuo browser in AWS CLI

1. Esegui il `list-assessments` comando per visualizzare un elenco delle tue valutazioni.

```
aws auditmanager list-assessments
```

   Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Esegui il `get-assessment` comando e specifica l'ID di valutazione sin dal primo passaggio.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Nella risposta, individua il set di controlli e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.
3. Esegui il `get-evidence-file-upload-url` comando e specifica il file che intendi caricare.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

   Nella risposta, prendere nota dell'URL predefinito e del `evidenceFileName`.
4. Utilizza l'URL predefinito del passaggio tre per caricare il file dal tuo browser. Questa azione carica il file su Amazon S3, dove viene salvato come oggetto che può essere allegato a un controllo di valutazione. Nel passaggio successivo, farai riferimento all'oggetto appena creato utilizzando il parametro `evidenceFileName`.

> **Note**
>
> Quando carichi un file utilizzando un URL predefinito, Audit Manager protegge e archivia i dati utilizzando la crittografia lato server con AWS Key Management Service. A tale scopo, è necessario utilizzare l'`x-amz-server-side-encryption` intestazione nella richiesta quando si utilizza l'URL predefinito per caricare il file. Se utilizzi un cliente gestito AWS KMS key nelle Configurazione delle impostazioni di crittografia dei dati impostazioni di Audit Manager, assicurati di includere anche l'`x-amz-server-side-encryption-aws-kms-key-id`intestazione nella richiesta. Se `x-amz-server-side-encryption-aws-kms-key-id` l'intestazione non è presente nella richiesta, Amazon S3 presuppone che l'utente voglia utilizzare la Chiave gestita da AWS.
> Per ulteriori informazioni, consulta Protezione dei dati utilizzando la crittografia lato server con AWS Key Management Service chiavi (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

5. Usa il `batch-import-evidence-to-assessment-control` comando con i parametri seguenti:

   - `--assessment-id`: usa l'ID di valutazione della prima fase.
   - `--control-set-id`: usa l'ID del set di controllo del secondo passaggio.
   - `--control-id`: usa l'ID di controllo del secondo passaggio.
   - `--manual-evidence`: utilizza `evidenceFileName` come tipo di prova manuale e specifica il nome del file delle prove nella fase tre.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Per caricare un file dal browser utilizzando l'API

1. Chiama `ListAssessments`l'operazione. Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Chiama `GetAssessment` l'operazione e specifica `assessmentId` dal primo passaggio. Nella risposta, individua il set di controlli e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.
3. Chiama l'`GetEvidenceFileUploadUrl` operazione e specifica `fileName` quello che vuoi caricare. Nella risposta, prendere nota dell'URL predefinito e del `evidenceFileName`.
4. Utilizza l'URL predefinito del passaggio tre per caricare il file dal tuo browser. Questa azione carica il file su Amazon S3, dove viene salvato come oggetto che può essere allegato a un controllo di valutazione. Nel passaggio successivo, farai riferimento all'oggetto appena creato utilizzando il parametro `evidenceFileName`.

   > **Note**
   >
   > Quando carichi un file utilizzando un URL predefinito, Audit Manager protegge e archivia i dati utilizzando la crittografia lato server con AWS Key Management Service. A tale scopo, è necessario utilizzare l'`x-amz-server-side-encryption` intestazione nella richiesta quando si utilizza l'URL predefinito per caricare il file.
   > Se utilizzi un cliente gestito AWS KMS key nelle Configurazione delle impostazioni di crittografia dei dati impostazioni di Audit Manager, assicurati di includere anche l'`x-amz-server-side-encryption-aws-kms-key-id`intestazione nella richiesta. Se `x-amz-server-side-encryption-aws-kms-key-id` l'intestazione non è presente nella richiesta, Amazon S3 presuppone che l'utente voglia utilizzare la Chiave gestita da AWS.
   > Per ulteriori informazioni, consulta Protezione dei dati utilizzando la crittografia lato server con AWS Key Management Service chiavi (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.
5. Chiama l'operazione `BatchImportEvidenceToAssessmentControl`con i parametri seguenti:
   - `assessmentId`: usa l'ID di valutazione della prima fase.
   - `controlSetId`: usa l'ID del set di controllo del secondo passaggio.

- `controlId`: usa l'ID di controllo del secondo passaggio.
- `manualEvidence`: utilizza `evidenceFileName` come tipo di prova manuale e specifica il nome del file delle prove nella fase tre.

Per ulteriori informazioni, scegli uno dei link nella procedura precedente per saperne di più nell'API Reference.AWS Audit Manager Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Dopo aver raccolto e esaminato le prove per la valutazione, puoi generare un rapporto di valutazione. Per ulteriori informazioni, consulta Preparazione di un rapporto di valutazione in AWS Audit Manager.

Altre risorse

Per sapere quali formati di file puoi usare, consultaFormati di file supportati per prove manuali.

Inserimento di risposte di testo in formato libero come prova manuale

È possibile fornire informazioni di contesto e di supporto aggiuntive per un controllo di valutazione inserendo testo in formato libero e salvandolo come prova. Ciò consente di documentare manualmente i dettagli che non vengono acquisiti tramite la raccolta automatica delle prove.

Ad esempio, è possibile utilizzare Audit Manager per creare controlli personalizzati che rappresentano domande in un questionario di valutazione del rischio del fornitore. In questo caso, il nome di ogni controllo è una domanda specifica che richiede informazioni sullo stato di sicurezza e conformità dell'organizzazione. Per registrare la risposta a una determinata domanda di valutazione del rischio del fornitore, è possibile inserire una risposta testuale e salvarla come prova manuale per il controllo.

Prerequisiti

- Quando un controllo è nello stato inattivo, non puoi aggiungere prove manuali relative a quel controllo. Per aggiungere prove manuali, è necessario innanzitutto modificare lo stato del controllo impostandolo su In revisione o in revisione.
- Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per gestire una valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni

sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile inserire risposte di testo utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

Per inserire una risposta di testo nella console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Valutazioni, quindi scegli una valutazione.
3. Scegli la scheda Controlli, scorri verso il basso fino a Set di controllo, quindi scegli un controllo.
4. Dalla scheda Cartelle delle prove, scegli Aggiungi prove manuali.
5. Scegli Inserisci risposta testuale.
6. Nella finestra pop-up che appare, inserisci la risposta in formato testo semplice.
7. Scegli Conferma.

AWS CLI

Nella procedura seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

Per inserire una risposta testuale nella AWS CLI

1. Esegui il comando `list-assessments`.

```
aws auditmanager list-assessments
```

   Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Esegui il `get-assessment` comando e specifica l'ID di valutazione sin dal primo passaggio.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Nella risposta, individua il set di controllo e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.

3. Usa il `batch-import-evidence-to-assessment-control` comando con i parametri seguenti:

   - `--assessment-id`: usa l'ID di valutazione della prima fase.
   - `--control-set-id`: usa l'ID del set di controllo del secondo passaggio.
   - `--control-id`: usa l'ID di controllo del secondo passaggio.
   - `--manual-evidence`: usa `textResponse` come tipo di prova manuale e inserisci il testo che desideri salvare come prova manuale.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Per inserire una risposta di testo utilizzando l'API

1. Chiama `ListAssessments`l'operazione. Nella risposta, trova la valutazione in cui desideri caricare le prove e prendi nota dell'ID della valutazione.
2. Chiama `GetAssessment` l'operazione e specifica `assessmentId` dal primo passaggio. Nella risposta, individua il set di controllo e il controllo su cui desideri caricare le prove e prendi nota dei relativi ID.
3. Chiama l'operazione `BatchImportEvidenceToAssessmentControl`con i parametri seguenti:

   - `assessmentId`: usa l'ID di valutazione della prima fase.
   - `controlSetId`: usa l'ID del set di controllo del secondo passaggio.
   - `controlId`: usa l'ID di controllo del secondo passaggio.

- `manualEvidence`: usa `textResponse` come tipo di prova manuale e inserisci il testo che desideri salvare come prova manuale.

Per ulteriori informazioni, scegliete uno dei collegamenti nella procedura precedente per saperne di più nell'AWS Audit Manager API Reference. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Dopo aver raccolto e esaminato le prove per la valutazione, puoi generare un rapporto di valutazione. Per ulteriori informazioni, consulta Preparazione di un rapporto di valutazione in AWS Audit Manager.

Formati di file supportati per prove manuali

Nella tabella seguente sono elencati e descritti i tipi di file che è possibile caricare come prova manuale. Per ogni tipo di file, la tabella elenca anche le estensioni di file supportate.

Tipo di file	Descrizione	Estensioni file supportate
Compressione o archiviazione	Archivi compressi GNU Zip e archivi compressi ZIP	`.gz`, `.zip`
Documento	File di documenti comuni come PDF e file di Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Immagine	File di immagini e grafici	`.jpeg`, `.jpg`, `.png`, `.svg`
Testo	Altri file di testo non binari, come documenti di testo semplice e file in linguaggio di markup	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Risorse aggiuntive

Consulta le pagine seguenti per scoprire i diversi modi in cui puoi aggiungere le tue prove a un controllo di valutazione.

- Importazione di file di prove manuali da Amazon S3
- Caricamento manuale di file di prove dal browser
- Inserimento di risposte di testo in formato libero come prova manuale

Preparazione di un rapporto di valutazione in AWS Audit Manager

Dopo aver raccolto ed esaminato le prove per la valutazione, puoi generare un rapporto di valutazione. Un rapporto di valutazione riassume la valutazione e fornisce collegamenti a un set organizzato di cartelle che contengono le prove correlate.

Punti chiave

Le prove appena raccolte non compaiono automaticamente in un rapporto di valutazione. Ciò significa che puoi controllare quali prove desideri includere nel rapporto. Dopo aver selezionato le prove da includere, puoi generare il rapporto di valutazione finale da condividere con i revisori.

Quando generi un report di valutazione, questo viene inserito nel bucket S3 che hai scelto come destinazione del report di valutazione. È inoltre possibile scaricare il rapporto di valutazione dal centro download di Audit Manager.

Risorse aggiuntive

Per ulteriori informazioni sui rapporti di valutazione e su come gestirli, consulta le seguenti risorse.

- Aggiungere prove a un report di valutazione
- Rimuovere le prove da un report di valutazione
- Generazione di un report di valutazione
- Scaricamento di un rapporto di valutazione
- Navigare in un rapporto di valutazione ed esplorarne il contenuto
- Convalida di un rapporto di valutazione
- Eliminazione di un report di valutazioni
- Generazione di report di valutazione dai risultati della ricerca di evidenze
- Configurazione della destinazione predefinita del rapporto di valutazione
- Risoluzione dei problemi relativi ai report di valutazione

Aggiungere prove a un report di valutazione

Per poter generare un report di valutazione, devi aggiungere almeno una prova al report di valutazione. Puoi aggiungere un'intera cartella di prove oppure aggiungere elementi di prova specifici dall'interno di una cartella.

Procedura

Per includere prove in un rapporto di valutazione, segui questi passaggi.

Aggiungere prove a un report di valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Valutazioni, quindi scegli una valutazione.
3. Nella scheda Controlli, scorri verso il basso fino alla tabella Set di controlli e scegli un controllo con le prove che desideri includere nel rapporto di valutazione.
4. Scegli come aggiungere prove al tuo report di valutazione.

    a. Per aggiungere un'intera cartella delle prove, scorri verso il basso fino a Cartelle delle prove, seleziona la cartella che desideri aggiungere, quindi scegli Aggiungi al report di valutazione.

    > **Tip**
    >
    > Se non riesci a vedere la cartella che stai cercando, modifica il filtro a discesa su Tutto il tempo. Altrimenti, per impostazione predefinita, verranno visualizzate le cartelle degli ultimi sette giorni.
    > Se l'opzione Aggiungi al report di valutazione è disattivata, la cartella delle prove è già stata aggiunta al report di valutazione.

    b. Per aggiungere prove specifiche, scegli una cartella delle prove per aprirne il contenuto. Seleziona uno o più elementi dall'elenco e scegli Aggiungi al report di valutazione.

    > **Tip**
    >
    > Se l'opzione Aggiungi al report di valutazione è disattivata, assicurati di aver selezionato la casella di controllo accanto alle prove, quindi riprova.

5. Dopo aver aggiunto le prove al report di valutazione, viene visualizzato un banner verde di successo. Scegli Visualizza le prove nel report di valutazione per visualizzare le prove che verranno incluse nel report di valutazione.
    - In alternativa, puoi visualizzare le prove che verranno incluse nel report di valutazione tornando alla valutazione e selezionando la scheda di selezione del report di valutazione.

Passaggi successivi

Se devi rimuovere delle prove da un rapporto di valutazione, consultaRimuovere le prove da un report di valutazione.

Quando sei pronto per generare un rapporto di valutazione, consultaGenerazione di un report di valutazione.

Risorse aggiuntive

Per trovare le risposte a domande e problemi comuni, Risoluzione dei problemi relativi ai report di valutazione consulta la sezione Risoluzione dei problemi di questa guida.

Rimuovere le prove da un report di valutazione

Se devi rimuovere prove da un report di valutazione, segui questi passaggi. È possibile rimuovere un'intera cartella di prove, oppure rimuovere elementi di prova specifici all'interno di una cartella.

Procedura

Per rimuovere le prove da un report di valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione scegli Valutazioni, quindi scegli il nome di una valutazione per aprirla.
3. Sulla scheda Controlli, scorri verso il basso fino alla tabella Set di controlli, quindi scegli il nome di un controllo per aprirlo.
4. Scegli come rimuovere le prove dal report di valutazione.
    a. Per rimuovere un'intera cartella delle prove, scorri verso il basso fino a Cartelle delle prove, seleziona la cartella che desideri rimuovere, quindi scegli Rimuovi dal report di valutazione.

> **Tip**
>
> Se non riesci a vedere la cartella che stai cercando, modifica il filtro a discesa su Tutto il tempo. Altrimenti, per impostazione predefinita, verranno visualizzate le cartelle degli ultimi sette giorni.
> Se l'opzione Rimuovi dal report di valutazione è disattivata, la cartella delle prove è già stata rimossa dal report di valutazione.

b. Per rimuovere prove specifiche, scegli una cartella delle prove per aprirne il contenuto. Seleziona uno o più elementi dall'elenco e scegli Rimuovi dal report di valutazione.

> **Tip**
>
> Se l'opzione Rimuovi dal report di valutazione è disattivata, assicurati di aver selezionato la casella di controllo accanto alle prove, quindi riprova.

5. Dopo aver aggiunto le prove al report di valutazione, viene visualizzato un banner verde di successo. Scegli Visualizza le prove nel report di valutazione per visualizzare le prove che verranno incluse nel report di valutazione.
   - In alternativa, puoi visualizzare le prove che verranno incluse nel report di valutazione tornando alla valutazione e selezionando la scheda di selezione del report di valutazione.

Passaggi successivi

Quando sei pronto per generare un rapporto di valutazione, consultaGenerazione di un report di valutazione.

Risorse aggiuntive

Per trovare le risposte a domande e problemi comuni, Risoluzione dei problemi relativi ai report di valutazione consulta la sezione Risoluzione dei problemi di questa guida.

Generazione di un report di valutazione

Quando sei pronto per generare il rapporto di valutazione, segui questi passaggi.

Prerequisiti

Per poter generare un report di valutazione, devi aggiungere almeno una prova al report di valutazione. Puoi aggiungere un'intera cartella di prove oppure aggiungere singoli elementi di prova dall'interno di una cartella.

Per assicurarti che il report di valutazione venga generato correttamente, consulta il nostro. Suggerimenti di configurazione per la destinazione del rapporto di valutazione

Procedura

Per generare un report di valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro sinistro di navigazione scegliere Esecuzioni di valutazione.
3. Scegliere il nome della valutazione per la quale si desidera generare un report di valutazione.
4. Scegli la scheda di selezione del report di valutazione, quindi scegli Genera report di valutazione.

   > **Tip**
   >
   > Se l'opzione 'Genera report di valutazione è disattivata, significa che non è stata ancora aggiunta alcuna prova al report di valutazione.

5. Nella finestra pop-up, fornisci un nome e una descrizione per il report di valutazione ed esamina i dettagli del report di valutazione.
6. Scegli Genera report di valutazione e attendi qualche minuto mentre viene generato il report di valutazione.
7. Trova e scarica il report di valutazione dalla pagina Download center della console Genera audit.
   - In alternativa, puoi accedere al bucket S3 di destinazione del report di valutazione e scaricare il report di valutazione da lì.

Passaggi successivi

Dopo aver creato un report di valutazione, è possibile ottenere ulteriori informazioni su:

- Trova e scarica il tuo report di valutazione: scopri come scaricare il report di valutazione dal centro download o da Amazon S3.

- Esplora il tuo report di valutazione: scopri come navigare in un report di valutazione ed esplorarne i contenuti.
- Convalida il rapporto di valutazione: scopri come utilizzare il funzionamento dell'ValidateAssessmentReportIntegrityAPI per convalidare il rapporto di valutazione.
- Eliminare un report di valutazione indesiderato: scopri come eliminare un report indesiderato dal centro download o da Amazon S3.
- Genera report di valutazione da Evidence Finder: scopri come generare report di valutazione dai risultati di ricerca del tuo Evidence Finder.

Risorse aggiuntive

Per trovare risposte a domande e problemi comuni, consulta Risoluzione dei problemi relativi ai report di valutazione la sezione Risoluzione dei problemi di questa guida.

Modifica dello stato di un controllo di valutazione in AWS Audit Manager

È possibile modificare lo stato di un controllo di valutazione all'interno della valutazione attiva. L'aggiornamento dello stato di un controllo consente di monitorarne l'avanzamento e indicare quando lo è stato esaminato, mantenendo la valutazione organizzata e up-to-date.

Prerequisiti

La procedura seguente presuppone che sia stata precedentemente creata una valutazione e che il suo stato attuale sia attivo.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per gestire una valutazione in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile aggiornare lo stato di controllo della valutazione utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Note**
>
> La modifica dello stato di controllo in Revisionato è definitiva. Dopo aver impostato lo stato di un controllo su Revisionato, non è più possibile modificare lo stato di tale controllo o ripristinare uno stato precedente.

Audit Manager console

Per modificare lo stato di controllo della valutazione sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Valutazioni.
3. Scegli il nome della valutazione per aprirla.
4. Per la pagina di valutazione, scegli la scheda Controlli, scorri verso il basso fino alla tabella Set di controlli, quindi seleziona il nome di un controllo per aprirlo.
5. Scegli Aggiorna stato di controllo in alto a destra della pagina, quindi scegli uno stato:

Stato	Descrizione
In fase di revisione	Scegli questo stato se non hai ancora esaminato il controllo.
Recensito	Scegli questo stato se hai finito di esaminare le prove per questo controllo e desideri continuare a raccogliere o aggiungere prove.
Inattivo	Scegli questo stato se non vuoi più raccogliere prove automatiche per questo controllo.

6. Scegli Aggiorna lo stato del controllo per confermare la tua scelta.

AWS CLI

Per modificare lo stato di controllo della valutazione in AWS CLI

1. Esegui il comando list-assessments.

```
aws auditmanager list-assessments
```

La risposta restituisce un elenco di valutazioni. Trova la valutazione che contiene il controllo che desideri aggiornare e prendi nota dell'ID della valutazione.

2. Esegui il comando get-assessment e specifica l'ID di valutazione dal passaggio 1.

   Nell'esempio seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
   ```

   Nella risposta, individua il controllo che desideri aggiornare e prendi nota dell'ID del controllo e dell'ID del relativo set di controlli.

3. Esegui il update-assessment-controlcomando e specifica i seguenti parametri:

   - `--assessment-id`— La valutazione a cui appartiene il controllo.
   - `--control-set-id`— Il set di controllo a cui appartiene il controllo.
   - `--control-id`— Il controllo che si desidera aggiornare.
   - `--control-status`— Imposta questo valore su `UNDER_REVIEWREVIEWED`, o`INACTIVE`.

   Nell'esempio seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

   ```
   aws auditmanager update-assessment-control --assessment-
   id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
   control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
   ```

Audit Manager API

Per modificare lo stato di controllo di una valutazione utilizzando l'API

1. Usa l'ListAssessmentsoperazione.

   Nella risposta, trova la valutazione che contiene il controllo che desideri aggiornare e prendi nota dell'ID della valutazione.

2. Usa l'GetAssessmentoperazione e specifica l'ID di valutazione del passaggio 1.

   Nella risposta, trova il controllo che desideri aggiornare e prendi nota dell'ID del controllo e dell'ID del relativo set di controlli.

3. Utilizzate l'UpdateAssessmentControloperazione e specificate i seguenti parametri:

   - `assessmentId`— La valutazione a cui appartiene il controllo.
   - `controlSetId`— Il set di controllo a cui appartiene il controllo.
   - `controlId`—Il controllo che si desidera aggiornare.
   - `controlStatus`— Imposta questo valore su `UNDER_REVIEWREVIEWED`, o`INACTIVE`.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nella Guida di riferimento all'AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Quando sei pronto a modificare lo stato della valutazione, consulta. Modificare lo stato di una valutazione in inattiva in AWS Audit Manager

Modificare lo stato di una valutazione in inattiva in AWS Audit Manager

Quando non è più necessario raccogliere prove per una valutazione, puoi modificare lo stato della valutazione in Inattivo. Quando lo stato di una valutazione diventa inattivo, la valutazione interrompe la raccolta delle prove. Di conseguenza, non ti verrà più addebitato alcun costo per tale valutazione.

Oltre a interrompere la raccolta delle prove, Gestione audit apporta le seguenti modifiche ai controlli inclusi nella valutazione inattiva:

- Tutti i set di controlli passano allo stato Revisionato.
- Tutti i controlli In fase di revisione passano allo stato Revisionato.
- I delegati alla valutazione inattiva non possono più visualizzare o modificare i controlli e i set di controlli.

Prerequisiti

La procedura seguente presuppone che tu abbia precedentemente creato una valutazione e che il suo stato attuale sia attivo.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per gestire una valutazione in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile aggiornare lo stato di valutazione utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Questa operazione è irreversibile. Ti consigliamo di procedere con cautela e di assicurarti di voler contrassegnare la valutazione come inattiva. Quando una valutazione è inattiva, è possibile accedere in sola lettura al contenuto. È comunque possibile visualizzare le prove raccolte in precedenza e generare report di valutazione. Tuttavia, non puoi modificare la valutazione inattiva, aggiungere commenti o caricare prove manuali.

Audit Manager console

Per modificare lo stato di valutazione in inattivo sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Valutazioni.
3. Scegli il nome della valutazione per aprirla.
4. Nell'angolo in alto a destra della pagina scegliere Aggiorna stato della valutazione, quindi scegliere Inattivo.
5. Scegli Aggiorna stato nella finestra pop-up per confermare che desideri modificare lo stato in inattivo.

Le modifiche alla valutazione e ai relativi controlli hanno effetto dopo circa un minuto.

AWS CLI

Per modificare lo stato di una valutazione in inattivo in AWS CLI

1. Innanzitutto, identifica la valutazione che intendi aggiornare. Per fare ciò, esegui il comando list-assessments.

```
aws auditmanager list-assessments
```

   La risposta restituisce un elenco di valutazioni. Trova la valutazione che desideri disattivare e prendi nota dell'ID della valutazione.

2. Quindi, esegui il update-assessment-statuscomando e specifica i seguenti parametri:

   - `--assessment-id`: usa questo parametro per specificare la valutazione che desiderate disattivare.
   - `--status`: imposta questo valore su `INACTIVE`.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111 --status INACTIVE
```

Le modifiche alla valutazione e ai relativi controlli hanno effetto dopo circa un minuto.

Audit Manager API

Per modificare lo stato di una valutazione in inattivo utilizzando l'API

1. Utilizza l'ListAssessmentsoperazione per trovare la valutazione che desideri disattivare e prendi nota dell'ID della valutazione.
2. Utilizzate l'UpdateAssessmentStatusoperazione e specificate i seguenti parametri:

   - assessmentId: usa questo parametro per specificare la valutazione che si desidera disattivare.
   - status: imposta questo valore su `INACTIVE`.

Le modifiche alla valutazione e ai relativi controlli hanno effetto dopo circa un minuto.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nella Guida di riferimento all'AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Quando sei sicuro di non aver più bisogno della valutazione inattiva, puoi ripulire il tuo ambiente Audit Manager eliminando la valutazione. Per istruzioni, consulta Eliminazione di una valutazione in AWS Audit Manager.

Eliminazione di una valutazione in AWS Audit Manager

Quando non è più necessaria una valutazione, è possibile eliminarla dal proprio ambiente Audit Manager. Ciò consente di ripulire lo spazio di lavoro e concentrarsi sulle valutazioni pertinenti alle attività e alle priorità attuali.

> **Tip**
>
> Se il tuo obiettivo è ridurre i costi, valuta la possibilità di modificare lo stato della valutazione in inattivo anziché eliminarla. Questa azione interrompe la raccolta delle prove e mette la valutazione in uno stato di sola lettura in cui è possibile rivedere le prove raccolte in precedenza. Le valutazioni inattive non comportano alcun costo.

Prerequisiti

La procedura seguente presuppone che sia stata precedentemente creata una valutazione.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per eliminare una valutazione in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile eliminare le valutazioni utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Questa azione elimina definitivamente la tua valutazione e tutte le prove che ha raccolto. Non puoi recuperare questi dati. Di conseguenza, ti consigliamo di procedere con cautela e di assicurarti di voler eliminare la valutazione.

Audit Manager console

Per eliminare una valutazione dalla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Valutazioni.
3. Selezionare la valutazione che si desidera eliminare e scegliere Elimina.

AWS CLI

Per eliminare una valutazione nel AWS CLI

1. Innanzitutto, identifica la valutazione che intendi eliminare. Per fare ciò, esegui il comando list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   La risposta restituisce un elenco di valutazioni. Trova la valutazione che desideri eliminare e prendi nota dell'ID della valutazione.
2. Quindi usa il comando delete-assessment e specifica il `--assessment-id` della valutazione che desideri eliminare.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Per eliminare una valutazione utilizzando l'API

1. Utilizza l'ListAssessmentsoperazione per trovare la valutazione che desideri eliminare.

   Nella risposta, prendere nota dell'ID di valutazione.
2. Utilizzate l'DeleteAssessmentoperazione e specificate l'AssessmentID della valutazione che desiderate eliminare.

Per ulteriori informazioni su queste operazioni API, scegli uno dei link precedenti per consultare il AWS Audit Manager Riferimento API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK AWS specifici della lingua.

Risorse aggiuntive

Per informazioni sulla conservazione dei dati in Audit Manager, vedereEliminazione dei dati di Gestione audit.

Delegazioni in AWS Audit Manager

Durante il processo di valutazione in AWS Audit Manager, potresti incontrare situazioni in cui hai bisogno dell'aiuto di esperti in materia per esaminare e convalidare le prove raccolte. È qui che entra in gioco il concetto di delegazione.

Punti chiave

Le deleghe consentono ai responsabili degli audit di assegnare set di controllo specifici ai delegati, persone con competenze specializzate nelle aree pertinenti. Utilizzando la funzione di delega, è possibile garantire che le prove relative a ciascun controllo vengano valutate a fondo dal personale appropriato. Ciò consente di semplificare il processo di revisione e migliorare l'accuratezza e l'affidabilità complessive delle valutazioni. Che abbiate bisogno di indicazioni sull'interpretazione delle prove tecniche, sul chiarimento dei requisiti di conformità o sull'acquisizione di informazioni più approfondite su domini specifici, le deleghe vi consentono di collaborare efficacemente con gli esperti in materia.

Ad alto livello, il processo di delega è il seguente:

1. Il proprietario dell'audit sceglie un set di controlli nella propria valutazione e lo delega per la revisione.
2. Il delegato esamina tali controlli e le relative evidenze e, una volta terminato, sottopone il controllo impostato al proprietario dell'audit.
3. Il proprietario dell'audit viene informato del completamento della revisione e verifica che i controlli esaminati non contengano eventuali osservazioni del delegato.

> **Note**
>
> An Account AWS può essere titolare di un audit o delegato in diversi modi Regioni AWS.

Risorse aggiuntive

Utilizza le seguenti sezioni di questo capitolo per ulteriori informazioni su come gestire le attività di delega in AWS Audit Manager.

Comprensione delle diverse attività di delega per i titolari di audit

In qualità di responsabile dell'audit AWS Audit Manager, sei responsabile della gestione delle valutazioni e della garanzia della conformità all'interno della tua organizzazione. Sebbene tu abbia esperienza in materia di governance, rischio e conformità, a volte potresti avere domande o aver bisogno dell'assistenza di esperti in materia per esaminare e interpretare prove o controlli tecnici specifici. È qui che diventa utile la funzionalità di delega in Audit Manager.

Punti chiave

La creazione di una delega consente di assegnare set di controllo all'interno di una valutazione ad altri utenti di Audit Manager (noti come delegati) che hanno conoscenze specialistiche o competenze tecniche nelle aree pertinenti. Questi delegati possono quindi esaminare i set di controllo assegnati, analizzare le prove raccolte, fornire commenti o prove aggiuntive, se necessario, e aggiornare lo stato dei singoli controlli.

Il processo di delega semplifica la revisione e la convalida dei controlli sfruttando l'esperienza collettiva all'interno dell'organizzazione. Garantisce che ogni controllo sia valutato a fondo dal personale più qualificato, migliorando l'accuratezza e l'affidabilità delle valutazioni.

Risorse aggiuntive

Le seguenti sezioni illustrano le diverse attività associate alla gestione delle deleghe in qualità di titolare dell'audit. Ciò include come delegare i set di controllo, tenere traccia dello stato delle deleghe

e gestire le deleghe completate. Utilizzando efficacemente le deleghe, è possibile collaborare con esperti in materia, sfruttare le loro conoscenze specialistiche e mantenere un processo di audit completo e ben informato all'interno di Audit Manager.

- Delegare un set di controllo per la revisione in AWS Audit Manager
- Individuazione e revisione delle delegazioni che hai inviato AWS Audit Manager
- Eliminazione delle delegazioni completate in AWS Audit Manager

Delegare un set di controllo per la revisione in AWS Audit Manager

Quando hai bisogno dell'assistenza di un esperto in materia, puoi scegliere Account AWS quello che desideri aiutarti e quindi delegare a lui un set di controllo per la revisione.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per creare una delega. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per delegare un set di controlli puoi utilizzare una delle seguenti procedure.

Delegare un set di controlli da una pagina di valutazione

Per delegare un set di controlli da una pagina di valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Valutazioni.
3. Seleziona il nome della valutazione che contiene il set di controlli che desideri delegare.
4. Dalla pagina di valutazione, scegli la scheda Controlli. Viene visualizzato il riepilogo dello stato del controllo e l'elenco dei controlli inclusi nella valutazione.
5. Seleziona un set di controlli e scegli Delega set di controlli.
6. Nella sezione Selezione delegati, viene visualizzato un elenco di utenti e ruoli. Scegli un utente o un ruolo oppure usa la barra di ricerca per cercarne uno.

7. Nella sezione Dettagli della delega, esamina il nome del set di controlli e il nome della valutazione.
8. (Facoltativo) Nella sezione Commenti, aggiungi un commento con le istruzioni per aiutare il delegato a svolgere il compito di revisione. Non includere informazioni sensibili nel tuo commento.
9. Scegli Delega set di controlli.
10. Un banner verde di successo conferma l'avvenuta delega del set di controlli. Scegli Visualizza delega per visualizzare la richiesta di delega. Puoi anche visualizzare le deleghe in qualsiasi momento selezionando Deleghe nel riquadro di navigazione a sinistra della console. AWS Audit Manager

Delegare un set di controlli dalla pagina delle deleghe

Per delegare un set di controlli dalla pagina delle deleghe

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Deleghe.
3. Dalla pagina delle deleghe, seleziona Crea delega.
4. Nella sezione Scegli il set di valutazione e controllo, specifica la valutazione e il set di controlli che desideri delegare.
5. Nella sezione Selezione delegati, vedrai un elenco di utenti e ruoli. Scegli un utente o un ruolo oppure usa la barra di ricerca per cercarne uno.
6. (Facoltativo) Nella sezione Commenti, aggiungi un commento con le istruzioni per aiutare il delegato a svolgere il compito di revisione. Non includere informazioni sensibili nel tuo commento.
7. Scegli Crea delega.
8. Un banner verde di successo conferma l'avvenuta delega del set di controlli. Scegli Visualizza delega per visualizzare la richiesta di delega. Puoi anche visualizzare le deleghe in qualsiasi momento selezionando Deleghe nel riquadro di navigazione a sinistra della console. AWS Audit Manager

Dopo aver delegato un set di controllo per la revisione, il delegato riceve una notifica e può quindi iniziare a rivedere il set di controllo. Questo processo seguito dai delegati è descritto in Comprensione delle diverse attività di delega per i delegati.

Passaggi successivi

Per rivedere la delegazione in un secondo momento, consulta. Individuazione e revisione delle delegazioni che hai inviato AWS Audit Manager

Individuazione e revisione delle delegazioni che hai inviato AWS Audit Manager

Puoi accedere a un elenco delle tue delegazioni in qualsiasi momento selezionando Deleghe nel riquadro di navigazione a sinistra di Audit Manager. La pagina delle deleghe contiene un elenco delle delegazioni attive e completate.

Quando una delega è completata, si riceve una notifica in Audit Manager. È inoltre possibile ricevere commenti con osservazioni dal delegato. La procedura seguente spiega come controllare le deleghe in Audit Manager dopo che sono state completate e come visualizzare eventuali commenti che il delegato potrebbe aver lasciato per voi.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare una delega. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Segui questi passaggi per trovare e rivedere le deleghe che hai creato in precedenza.

Per visualizzare una delega completata e verificare la presenza di commenti

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Deleghe.
3. Consulta la pagina Deleghe, che include una tabella con le seguenti informazioni:

Nome	Descrizione
Delegato a	La persona a Account AWS cui hai delegato il set di controllo.
Data	La data in cui hai delegato il set di controllo.
Stato	Lo stato attuale della delega.
Valutazione	Il nome della valutazione con un collegamento alla pagina dei dettagli della valutazione.
Set di controllo	Il nome del set di controlli che è stato delegato per la revisione.

4. Trova il set di valutazione e controllo che il delegato ha esaminato e inviato a te e scegli il nome della valutazione per aprirlo.
5. Nella sezione Controlli della pagina dei dettagli della valutazione, scorri verso il basso fino alla tabella Impostazioni controlli.
6. In Controlli raggruppati per set di controlli, trova il nome del set di controlli che hai delegato.
7. Espandi il nome del set di controlli per mostrarne i controlli e scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
8. Scegli la scheda Commenti per visualizzare eventuali commenti aggiunti dal delegato per quel particolare controllo.
9. Quando ritieni che la revisione di un set di controlli sia completa, seleziona il set di controlli e scegli Revisione completa del set di controlli.

Important

Gestione audit raccoglie prove in modo continuo. Di conseguenza, potrebbero essere raccolte nuove prove aggiuntive dopo che il delegato ha completato la revisione di un controllo.
Se desideri utilizzare solo le prove esaminate nei rapporti di valutazione, puoi fare riferimento al timestamp della revisione del controllo per determinare quando le prove sono state esaminate. Questo timestamp è disponibile nella pagina Scheda Changelog dei dettagli del controllo. Puoi quindi utilizzare questo timestamp per identificare quali prove aggiungere ai rapporti di valutazione.

Passaggi successivi

Per eliminare una delega dopo che è stata completata e non è più necessaria, consulta. Eliminazione delle delegazioni completate in AWS Audit Manager

Eliminazione delle delegazioni completate in AWS Audit Manager

In alcuni casi è possibile che si crei una delega ma in seguito non sia più necessaria assistenza per la revisione del set di controlli. Quando ciò accade, è possibile eliminare una delega attiva in Audit Manager. È inoltre possibile eliminare le deleghe completate che non si desidera più visualizzare nella pagina delle deleghe.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per eliminare una delega in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per eliminare una delega

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona Deleghe.
3. Nella pagina Deleghe, seleziona la delega che desideri annullare, quindi scegli Rimuovi delega.
4. Nella finestra a comparsa, scegli Elimina per confermare la scelta.

Comprensione delle diverse attività di delega per i delegati

In qualità di delegato AWS Audit Manager, svolgi un ruolo importante nel supportare i titolari degli audit durante il processo di valutazione. Sebbene i titolari degli audit siano responsabili della gestione delle valutazioni e della garanzia della conformità generale, a volte potrebbero aver bisogno dell'assistenza di esperti in materia per la revisione e l'interpretazione di prove tecniche specifiche che non rientrano nelle loro aree di competenza. In tali scenari, le conoscenze e le competenze acquisiscono un valore inestimabile.

Punti chiave

La funzione di delega consente ai responsabili dell'audit di assegnare all'utente set di controllo specifici per la revisione, attingendo alle competenze aziendali o tecniche specializzate. Questo approccio collaborativo non solo migliora l'accuratezza e l'affidabilità delle valutazioni, ma semplifica anche il processo di revisione, consentendo ai responsabili degli audit di concentrarsi sulle loro responsabilità principali mentre voi concentrate i vostri sforzi sulle aree in cui la vostra esperienza è più preziosa.

In qualità di delegato, potreste ricevere richieste dai titolari degli audit per esaminare le prove associate ai set di controllo assegnati. Puoi aiutare i responsabili dell'audit esaminando i set di controlli e le relative evidenze aggiungendo commenti, caricando prove ulteriori e aggiornando lo stato di ogni controllo esaminato.

> **Note**
>
> I proprietari degli audit delegano specifici set di controlli per la revisione e non intere valutazioni. Di conseguenza, i delegati hanno un accesso limitato alle valutazioni. I delegati possono esaminare le prove, aggiungere commenti, caricare prove manuali e aggiornare lo stato di controllo per ciascuno dei controlli del set di controlli. Per ulteriori informazioni sui ruoli e autorizzazioni in Gestione audit, consulta Politiche consigliate per gli utenti in AWS Audit Manager.

Risorse aggiuntive

Nelle sezioni seguenti, è possibile ottenere ulteriori informazioni sulle attività associate alla gestione delle deleghe in qualità di delegato. Ciò include come visualizzare le richieste di delega in arrivo, rivedere i set di controllo assegnati, fornire commenti e prove aggiuntive e inviare i controlli esaminati al proprietario dell'audit.

- Visualizzazione delle notifiche per le richieste di delega in arrivo
- Revisione di un set di controlli e le relative prove
- Aggiungere commenti su un controllo durante la revisione di un set di controlli
- Contrassegnare un controllo come esaminato in AWS Audit Manager
- Invio di un set di controllo revisionato al titolare dell'audit

Visualizzazione delle notifiche per le richieste di delega in arrivo

Quando il proprietario di un audit richiede l'assistenza dell'utente per la revisione di un set di controlli, riceve una notifica che lo informa del set di controlli che gli è stato delegato.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare le notifiche. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per visualizzare le notifiche

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione sinistro, seleziona Notifiche.
3. Nella pagina Notifiche, esamini l'elenco dei set di controlli che ti sono stati delegati per la revisione. La tabella include le informazioni seguenti:

Nome	Descrizione
Data	La data in cui il set di controllo è stato delegato.
Valutazione	Il nome della valutazione associata al set di controlli.
Set di controllo	Il nome del set di controllo.
Origine	L'utente o il ruolo che ti ha delegato il set di controllo.
Descrizione	Istruzioni fornite dal titolare dell'audit.

> **Tip**
>
> Puoi anche iscriverti a un argomento SNS per ricevere avvisi e-mail quando ti viene delegato un set di controlli per la revisione. Per ulteriori informazioni, consulta Notifiche in AWS Audit Manager.

Passaggi successivi

Quando sei pronto per iniziare a rivedere i controlli che ti sono stati delegati, consultaRevisione di un set di controlli e le relative prove.

Revisione di un set di controlli e le relative prove

Puoi aiutare i responsabili dell'audit esaminando i set di controlli che ti hanno delegato.

Esaminando i controlli e le relative prove, puoi stabilire se sono necessarie ulteriori azioni. Tali azioni aggiuntive potrebbero includere il caricamento manuale di prove aggiuntive per dimostrare la conformità o l'inserimento di un commento che descriva in dettaglio le fasi di correzione seguite.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare un set di controlli. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Revisione di un set di controlli

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione, seleziona Notifiche.
3. Nella pagina Notifiche, puoi visualizzare un elenco di set di controlli che ti sono stati delegati. Identifica il set di controlli da esaminare e scegli il nome della valutazione correlata per aprire la pagina dei dettagli della valutazione.
4. Nella sezione Controlli della pagina dei dettagli della valutazione, scorri verso il basso fino alla tabella Impostazioni controlli.

5. Nella colonna Controlli raggruppati per set di controlli, espandi il nome di un set di controlli per mostrarne i controlli.
6. Scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
7. (Facoltativo) Scegli Aggiorna stato del controllo per modificare lo stato del controllo. Durante la revisione, puoi contrassegnare lo stato come In fase di revisione.
8. Consulta le informazioni sul controllo nelle schede Cartelle Evidence, Dettagli, Origini dati, Commenti e Changelog.

   - Per ulteriori informazioni su ciascuna di queste schede e su come comprendere i dati in esse contenuti, consulta. Revisione di un controllo di valutazione in AWS Audit Manager

Per esaminare le prove per un controllo

1. Dalla pagina dei dettagli del controllo, scegli la scheda Cartelle di prove.
2. Vai alla tabella delle cartelle Evidence per visualizzare un elenco di cartelle che contengono le prove relative a tale controllo. Queste cartelle sono organizzate e denominate in base alla data in cui sono state raccolte le prove.
3. Scegli il nome di una cartella di prove per aprirla. Pertanto, puoi consultare un riepilogo di tutte le prove raccolte in quella data.

   - Questo riepilogo include il numero totale di problemi di controllo di conformità segnalati direttamente da AWS Security Hub o da entrambi. AWS Config
   - Per ulteriori informazioni su queste informazioni, vedereRevisione di una cartella di prove in AWS Audit Manager.
4. Dalla pagina di riepilogo della cartella delle prove, vai alla tabella Prove. Nella colonna Ora, scegli una prova da aprire.
5. Esamina i dettagli delle prove.

   - Per ulteriori informazioni su queste informazioni, vedereRevisione delle prove in AWS Audit Manager.

Passaggi successivi

In alcuni casi potrebbe essere necessario fornire prove aggiuntive per dimostrare la conformità. In questi casi puoi caricare manualmente le prove. Per istruzioni, consulta Aggiungere prove manuali in AWS Audit Manager.

Se desideri lasciare commenti su uno o più controlli che ti sono stati delegati, consultaAggiungere commenti su un controllo durante la revisione di un set di controlli.

Aggiungere commenti su un controllo durante la revisione di un set di controlli

Puoi aggiungere commenti per tutti i controlli che esamini. Questi commenti sono visibili al proprietario dell'audit.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per aggiungere commenti a un controllo di valutazione. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per aggiungere un commento a un controllo

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione sinistro, seleziona Notifiche.
3. Nella pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati.
4. Trova il set di controlli che contiene il controllo per il quale desideri lasciare un commento, quindi scegli il nome della valutazione correlata per aprire la valutazione.
5. Scegli la scheda Controlli, scorri verso il basso fino alla tabella Set di controlli, quindi seleziona il nome di un controllo per aprirlo.
6. Scegli la scheda Commenti.
7. Nella sezione Invia commenti, inserisci il tuo commento nella casella di testo.
8. Scegli Invia commento per aggiungere il tuo commento. Il tuo commento viene quindi visualizzato nella sezione Commenti precedenti della pagina, insieme a qualsiasi altro commento relativo a questo controllo.

Passaggi successivi

Una volta terminata la revisione del controllo, segui i passaggi indicatiContrassegnare un controllo come esaminato in AWS Audit Manager.

Contrassegnare un controllo come esaminato in AWS Audit Manager

È possibile indicare l'avanzamento della revisione aggiornando lo stato dei singoli controlli all'interno di un set di controlli.

La modifica dello stato di un controllo è facoltativa. Tuttavia, ti consigliamo di modificare lo stato di ogni controllo e impostarlo su Revisionato una volta completata la revisione di quel controllo. Indipendentemente dallo stato di ogni singolo controllo, puoi comunque restituire i controlli al proprietario dell'audit.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per aggiornare lo stato di controllo della valutazione in AWS Audit Manager. Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per contrassegnare un controllo come revisionato

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione sinistro, seleziona Notifiche.
3. Nella pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati.
4. Trova il set di controlli che desideri contrassegnare come revisionato, quindi scegli il nome della valutazione correlata per aprire la valutazione.
5. Nella sezione Controlli della pagina dei dettagli della valutazione, scorri verso il basso fino alla tabella Impostazioni controlli.
6. Nella colonna Controlli raggruppati per set di controlli, espandi il nome di un set di controlli per mostrarne i controlli.
7. Scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.

8. Scegli Aggiorna lo stato del controllo e modifica lo stato impostandolo su Revisionato.
9. Nella finestra pop-up che appare, scegli Aggiorna lo stato del controllo per confermare di aver terminato la revisione del controllo.

Passaggi successivi

Per completare il processo di delega, consultaInvio di un set di controllo revisionato al titolare dell'audit.

Invio di un set di controllo revisionato al titolare dell'audit

Dopo aver esaminato il set di controlli, aggiunto commenti o prove aggiuntive e aggiornato lo stato dei singoli controlli, si giunge a un passaggio importante: la restituzione del set di controllo esaminato al proprietario dell'audit. L'invio del set di controllo esaminato segna il completamento delle attività delegate e consente al proprietario dell'audit di incorporare le informazioni e i consigli dell'utente nella valutazione complessiva.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per inviare il set di controllo esaminato al titolare dell'audit in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager e. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Segui questi passaggi per inviare il set di controllo al proprietario dell'audit.

Per restituire un set di controlli revisionato al proprietario dell'audit

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione sinistro, seleziona Notifiche.
3. Esamina l'elenco dei set di controlli che ti sono stati delegati. Trova il set di controlli che desideri restituire al proprietario dell'audit e scegli il nome della valutazione correlata.
4. Scorri verso il basso fino alla tabella Set di controlli, seleziona il set di controlli che desideri inviare al proprietario dell'audit, quindi scegli Invia per una revisione.

5. Nella finestra pop-up che appare, puoi aggiungere commenti prima di scegliere Invia per una revisione.

Report di valutazione

Un report di valutazione riassume le prove selezionate che sono state raccolte per una valutazione. Contiene inoltre collegamenti a file PDF con dettagli su ogni elemento di prova. I contenuti specifici, l'organizzazione e la convenzione di denominazione di un report di valutazione dipendono dai parametri scelti al momento della generazione del report.

I report di valutazione aiutano l'utente a selezionare e compilare le prove pertinenti per l'audit. Tuttavia, non valutano la conformità delle prove stesse. Al contrario, Gestione audit fornisce semplicemente i dettagli delle prove selezionate come output che è possibile condividere con il revisore.

Indice

Comprensione della struttura delle cartelle del rapporto di valutazione

Quando si scarica un report di valutazione, Gestione audit produce una cartella zip. che contiene il report di valutazione e i relativi file di prove in sottocartelle annidate.

La cartella è strutturata come segue:

- Cartella di valutazione (esempio: `myAssessmentName-a1b2c3d4`): La cartella principale.
  - Cartella del rapporto di valutazione (esempio:`reportName-a1b2c3d4e5f6g7`): una sottocartella in cui è possibile trovare i AssessmentReportSummary file.pdf, digest.txt e README.txt.
    - Cartella Prove per controllo (esempio: `controlName-a1b2c3d4e5f6g`): Una sottocartella che raggruppa i file delle prove in base al controllo correlato.
      - Prove per cartella di origine dati (esempio: `CloudTrail`,`Security Hub`): Una sottocartella che raggruppa i file di prove in base al tipo di origine dati.
        - Cartella Prove per data (esempio: `2022-07-01`): Una sottocartella che raggruppa i file di prove in base alla data di raccolta.
          - File di prove: i file che contengono dettagli sui singoli elementi di prova.

Navigazione in un rapporto di valutazione

Inizia aprendo la cartella zip e navigando di un livello verso il basso fino alla cartella del report di valutazione. Qui puoi trovare il report di valutazione in PDF e il file README.txt.

È possibile esaminare il file README.txt per comprendere la struttura e il contenuto della cartella zip. Fornisce inoltre informazioni di riferimento sulle convenzioni di denominazione per ogni file. Queste informazioni possono aiutarti ad accedere direttamente a una sottocartella o a un file di prove se stai cercando un elemento specifico.

Altrimenti, per sfogliare le prove e individuare le informazioni di cui hai bisogno, apri il PDF del report di valutazione. Questo ti offre una panoramica di alto livello del report e un riepilogo della valutazione da cui è stato creato il report.

Successivamente, utilizza il sommario (TOC, table of contents) per esplorare il report. Puoi scegliere qualsiasi controllo con collegamento ipertestuale nel sommario per passare direttamente a un riepilogo di quel controllo.

Quando si è pronti a esaminare i dettagli delle prove per un controllo, è possibile farlo scegliendo il nome della prova con collegamento ipertestuale. Per le prove automatizzate, il collegamento ipertestuale apre un nuovo file PDF con i dettagli relativi a tali prove. Per le prove manuali, il collegamento ipertestuale ti porta al bucket S3 che contiene le prove.

> **Tip**
>
> Il percorso di navigazione nella parte superiore di ogni pagina mostra la tua posizione attuale nel report di valutazione mentre sfogli i controlli e le prove. Seleziona il relativo collegamento ipertestuale per tornare al sommario in qualsiasi momento.

Revisione delle sezioni di un rapporto di valutazione

Utilizza le seguenti informazioni per saperne di più su ciascuna sezione di un report di valutazione.

> **Note**
>
> Il trattino (-) accanto a uno qualsiasi degli attributi nelle sezioni seguenti indica che il valore di quell'attributo è nullo o che non esiste.

Frontespizio

Il frontespizio include il nome del report di valutazione. Visualizza anche la data e l'ora in cui è stato generato il report, insieme all'ID account dell'utente che lo ha generato.

Il frontespizio è formattato come segue. Gestione audit sostituisce i *`segnaposto`* con le informazioni pertinenti al report.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Pagina di panoramica

La pagina di panoramica è composta da due parti: un riepilogo del report stesso e un riepilogo della valutazione oggetto del report.

Riepilogo del report

Questa sezione riepiloga il report di valutazione.

Nome	Descrizione
Nome del rapporto	Il nome del report.
Descrizione	La descrizione inserita dal titolare dell'audit quando genera il rapporto.
Data di generazione	La data in cui è stato generato il rapporto. L'ora è presentata in formato UTC (Universal Time Code, codice orario universale).
Controlli totali inclusi	Il numero di controlli inclusi nel rapporto e che hanno raccolto prove. Si tratta di un sottoinsieme del numero totale di controlli inclusi nella valutazione.
Account AWS incluso	Il numero Account AWS di questi sono inclusi nel rapporto e hanno raccolto prove. Si tratta di un sottoinsieme del numero totale di partecipanti Account AWS alla valutazione.
Selezione del rapporto di valutazione	Il numero di elementi probatori selezionati per l'inclusione nel rapporto. Ciò include il numero totale di problemi di controllo della conformità rilevati nel report.

Riepilogo della valutazione

Questa sezione riepiloga la valutazione a cui si riferisce il report.

Nome	Descrizione
Nome della valutazione	Il nome della valutazione da cui è stato generato il rapporto.
Stato	Lo stato della valutazione nel momento in cui è stato generato il rapporto.
Regione di valutazione	La in Regione AWS cui è stata creata la valutazione.
Account AWS nell'ambito	L'elenco Account AWS di questi elementi rientra nell'ambito della valutazione.
Nome del framework	Il nome del framework da cui è stata creata la valutazione.
Proprietari dell'audit	L'utente o il ruolo dei titolari dell'audit della valutazione.
Ultimo aggiornamento	La data dell'ultimo aggiornamento della valutazione. L'ora è rappresentata in UTC.

Pagina del sommario

Il sommario mostra il contenuto completo del report di valutazione. I contenuti sono raggruppati e organizzati in base ai set di controllo inclusi nella valutazione. I controlli sono elencati sotto il rispettivo set di controlli.

Scegli qualsiasi elemento nel sommario per accedere direttamente a quella sezione del report. È possibile scegliere un set di controlli o passare direttamente a un controllo.

Pagina di controllo

La pagina di controllo è composta da due parti: un riepilogo del controllo stesso e un riepilogo delle prove raccolte per il controllo.

Riepilogo del controllo

Questa sezione include le seguenti informazioni.

Nome	Descrizione
Nome del controllo	Il nome del controllo.
Descrizione	Descrizione del controllo.
Set di controllo	Il nome del set di controlli a cui appartiene il controllo.
Informazioni sul test	Le procedure di test consigliate per questo controllo.
Piano d'azione	Le azioni consigliate da eseguire se il controllo non viene soddisfat to.
Selezione del rapporto di valutazione	Il numero di elementi probatori relativi a questo controllo che sono stati inclusi nel rapporto di valutazione. Ciò include il numero di problemi di verifica della conformità riscontrati riferiti alle prove relative a questo controllo.

Prove raccolte

Questa sezione mostra le prove raccolte per il controllo. Le prove sono raggruppate in cartelle, organizzate e denominate in base alla data di raccolta. Accanto al nome di ogni cartella di prove è riportato il numero totale di problemi di controllo della conformità per quella cartella.

Sotto il nome di ogni cartella di prove è presente un elenco di nomi di prove con collegamenti ipertestuali.

- I nomi automatici delle prove iniziano con un timestamp di raccolta delle prove, seguito da codice di servizio, nome dell'evento (fino a 20 caratteri), ID dell'account e da un ID univoco di 12 caratteri.

  Ad esempio: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Per le prove automatiche, il nome con collegamento ipertestuale apre un nuovo file PDF con un riepilogo e ulteriori dettagli.
- I nomi delle prove manuali iniziano con un timestamp di caricamento delle prove, seguito dall'etichetta, dall'ID dell'account e da un ID univoco di 12 caratteri di `manual`. Includono inoltre i primi 10 caratteri del nome del file e la sua estensione (fino a 10 caratteri).

  Ad esempio: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

Per le prove manuali, il collegamento ipertestuale porta al bucket S3 che contiene le prove.

Accanto a ciascuna prova è riportato il nome del risultato del controllo di conformità relativo a quell'elemento.

- Per le prove automatizzate raccolte da AWS Security Hub o AWS Config, viene riportato un risultato conforme, non conforme o non conclusivo.
- Per le prove automatiche raccolte da chiamate API AWS CloudTrail e per tutte le prove manuali, viene mostrato un risultato non conclusivo.

Pagina di riepilogo delle prove

La pagina di riepilogo delle prove include le seguenti informazioni.

Nome	Descrizione
ID	L'identificatore univoco delle prove.
Data raccolta	La data in cui le prove sono state create o caricate.
Descrizione	Una descrizione delle prove, inclusi l'ID dell'account e il tipo di fonte dei dati.
Nome della valutazione	Il nome della valutazione da cui è stato generato il rapporto.
Nome del framework	Il nome del framework da cui è stata creata la valutazione.
Nome del controllo	Il nome del controllo supportato dalle prove.
Nome del set di controlli	Il nome del set di controlli a cui appartiene il controllo correlato.
Descrizione del controllo	La descrizione del controllo supportata dalle prove.
Informazioni sui test	Le procedure di test consigliate per il controllo.
Piano d'azione	Le azioni consigliate da eseguire in caso di mancato rispetto del controllo.

Nome	Descrizione
Regione AWS	Il nome della regione associata alle prove.
ID IAM	L'ARN dell'utente o del ruolo associato alle prove.
Account AWS	L' Account AWS ID associato alle prove.
Servizio AWS	Il nome della Servizio AWS persona associata alla prova.
Nome evento	Il nome dell'evento probatorio.
Event time (Ora evento)	L'ora in cui si è verificato l'evento probatorio.
Origine dati	Da dove sono state raccolte o caricate le prove. Il tipo di origine dati può essere AWS Config Security Hub CloudTrail, chiamate AWS API o Manuale.
Prove per tipo	La categoria delle prove • Le prove del controllo di conformità vengono raccolte dal AWS Config nostro Security Hub. • Le prove dell'attività degli utenti vengono raccolte dai CloudTrail log. • Le prove dei dati di configurazione vengono raccolte da istantane e di altri. Servizi AWS • Le prove manuali sono prove che vengono caricate manualmen te.
Stato del controllo di conformità	Lo stato di valutazione delle prove che rientrano nella categoria del controllo di conformità. • Per le prove automatizzate raccolte da AWS Security Hub o AWS Config, viene riportato un risultato conforme, non conforme o non conclusivo. • Per le prove automatiche raccolte da chiamate API AWS CloudTrail e per tutte le prove manuali, viene mostrato un risultato non conclusivo.

Pagina dei dettagli delle prove

La pagina dei dettagli delle prove mostra il nome delle prove e una tabella dei dettagli delle prove. Questa tabella fornisce una suddivisione dettagliata di ogni elemento probatorio in modo da poter comprendere i dati e verificarne la correttezza. A seconda dell'origine dati delle prove, il contenuto della pagina di dettaglio varia.

> **Tip**
>
> Il percorso di navigazione nella parte superiore di ogni pagina mostra la posizione attuale dell'utente mentre sfoglia i dettagli delle prove. Seleziona Riepilogo delle prove per tornare al riepilogo delle prove in qualsiasi momento.

Convalida di un rapporto di valutazione

Quando si genera un report di valutazione, Gestione audit produce un checksum del file di report denominato`digest.txt`. Questo file può essere utilizzato per convalidare l'integrità del report e garantire che nessuna prova sia stata modificata dopo la sua creazione. Contiene un oggetto JSON con firme e hash che vengono invalidati se una qualsiasi parte dell'archivio del report viene alterata.

Per convalidare l'integrità di un rapporto di valutazione, utilizza l'ValidateAssessmentReportIntegrityAPI fornita da Audit Manager.

Risorse aggiuntive

Per trovare le risposte alle domande e ai problemi più comuni, consulta Risoluzione dei problemi relativi ai report di valutazione la sezione Risoluzione dei problemi di questa guida.

Evidence finder

Evidence finder offre un modo efficace per cercare prove in Gestione audit. Invece di sfogliare cartelle di prove racchiuse in profondità, per trovare ciò che stai cercando ora puoi utilizzare evidence finder per interrogare rapidamente le prove. Se utilizzi evidence finder come amministratore delegato, puoi cercare prove in tutti gli account dei membri della tua organizzazione.

Utilizzando una combinazione di filtri e raggruppamenti, è possibile restringere progressivamente l'ambito della query di ricerca. Ad esempio, se desideri una visione di alto livello dello stato del sistema, esegui una ricerca ampia e filtra per valutazione, intervallo di date e conformità delle risorse. Se il tuo obiettivo è correggere una risorsa specifica, puoi eseguire una ricerca ristretta per individuare le prove relative a un controllo o a un ID di risorsa specifico. Dopo aver definito i filtri, puoi raggruppare e visualizzare in anteprima i risultati di ricerca corrispondenti prima di creare un rapporto di valutazione.

Per utilizzare evidence finder, è necessario abilitare questa funzionalità dalle impostazioni di Gestione audit.

Punti chiave

Capire come funziona Evidence Finder con Lake CloudTrail

Evidence finder utilizza la funzionalità di interrogazione e archiviazione di Data Lake AWS CloudTrail. Prima di iniziare a utilizzare Evidence Finder, è utile capire qualcosa in più su come funziona CloudTrail Lake.

CloudTrail Lake aggrega i dati in un unico archivio di dati di eventi ricercabile che supporta potenti query SQL. Ciò significa che puoi cercare dati all'interno dell'organizzazione e all'interno di intervalli di tempo personalizzati. Con evidence finder, puoi utilizzare questa funzionalità di ricerca direttamente nella console Gestione audit.

Quando richiedi di abilitare evidence finder, Gestione audit crea un archivio di dati degli eventi per tuo conto. Una volta abilitato evidence finder, tutte le prove future di Gestione audit vengono inserite nell'archivio di dati degli eventi, dove sono disponibili per le query di ricerca dell'evidence finder. Dopo aver abilitato evidence finder, riempiamo anche il nuovo archivio di dati degli eventi con i dati relativi alle prove degli ultimi due anni. Se abiliti evidence finder come amministratore delegato, eseguiamo il riempimento dei dati per tutti gli account dei membri della tua organizzazione.

Tutti i dati relativi alle prove, nuovi o ripristinati, vengono conservati nell'archivio dati degli eventi per 2 anni. È possibile modificare il periodo di conservazione predefinito in qualsiasi momento. Per istruzioni, consulta Aggiornamento di un archivio di dati degli eventi nella Guida per l'utente AWS CloudTrail . Puoi conservare i dati dell'evento in un archivio di dati degli eventi per un massimo di 7 anni o 2.555 giorni.

> **Note**
>
> Quando vengono aggiunti nuovi dati di evidenza all'Event Data Store, vengono addebitati i costi di CloudTrail Lake per l'archiviazione e l'ingestione dei dati.
> Per le richieste su CloudTrail Lake, si paga in base al consumo. Ciò significa che per ogni query di ricerca che esegui in evidence finder, ti vengono addebitati i costi per i dati scansionati.
> Per ulteriori informazioni sui prezzi di CloudTrail Lake, consulta la pagina AWS CloudTrail dei prezzi.

Passaggi successivi

Per iniziare, abilita lo strumento di ricerca delle prove dalle impostazioni di Audit Manager. Per istruzioni, consulta Attivazione di evidence finder.

Risorse aggiuntive

- Ricerca di prove in Evidence Finder
- Visualizzazione dei risultati in evidence finder
- Opzioni di filtro e raggruppamento per Evidence Finder
- Esempi di casi d'uso per Evidence Finder
- Risoluzione dei problemi in Evidence Finder

Ricerca di prove in Evidence Finder

Puoi utilizzare Evidence Finder per eseguire ricerche mirate e individuare rapidamente le prove pertinenti da esaminare.

In questa pagina, imparerai come filtrare le tue ricerche in base a criteri quali valutazione, intervallo di date, stato di conformità delle risorse e attributi aggiuntivi. L'applicazione di questi filtri restringe l'ambito di ricerca alle sole prove di cui hai bisogno. Puoi anche raggruppare i risultati in base a determinati campi per analizzare meglio i modelli.

Prerequisiti

Assicurati di aver completato i passaggi per abilitare lo strumento di ricerca delle prove nelle impostazioni di Audit Manager. Per istruzioni, consulta Attivazione di evidence finder.

Inoltre, assicurati di disporre delle autorizzazioni per eseguire query di ricerca in Evidence Finder. Per un esempio di politica di autorizzazione che puoi utilizzare, vedi. Consenti agli utenti di eseguire query di ricerca in Evidence Finder

Procedura

Segui questi passaggi per cercare prove nella console Gestione audit.

1. Eseguire una query di ricerca
2. Interrompere una query di ricerca in corso (opzionale)
3. Modifica i filtri per la tua query di ricerca (opzionale)

> **Note**
>
> Puoi anche utilizzare l' CloudTrail API per interrogare i dati relativi alle prove. Per ulteriori informazioni, StartQueryconsulta l'AWS CloudTrail API Reference. Se preferisci utilizzare il AWS CLI, consulta Avvio di una query nella Guida per l'AWS CloudTrail utente.

Esecuzione di una query di ricerca

Segui questi passaggi per eseguire una query di ricerca in evidence finder.

Ricerca delle prove

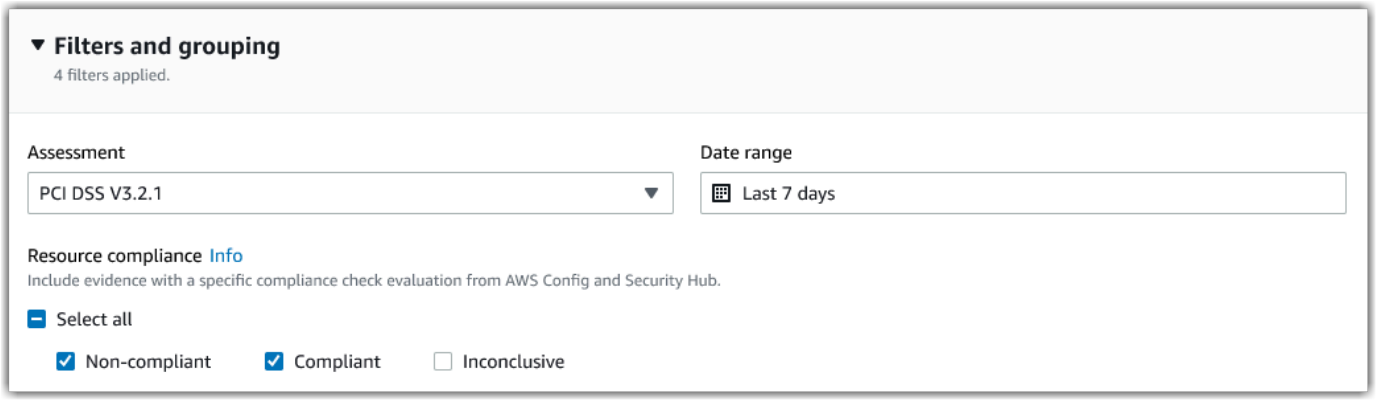
1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, seleziona evidence finder.

3. Successivamente, applica i filtri per restringere l'ambito della ricerca.

   a. Per Valutazione, scegli una valutazione.

   b. Per Intervallo di date, seleziona un intervallo.

   c. Per Conformità delle risorse, seleziona uno stato di valutazione.

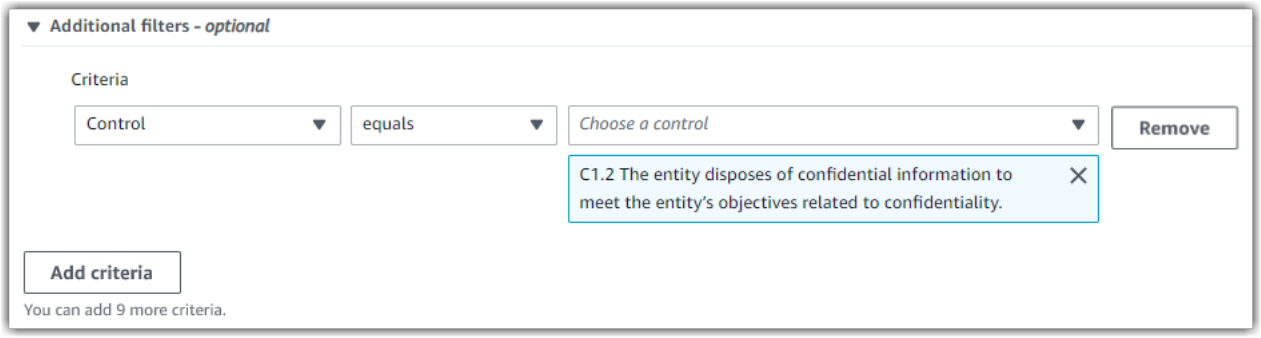


4. (Facoltativo) Scegli Filtri aggiuntivi: facoltativo per restringere ulteriormente la ricerca.

   a. Scegli Aggiungi criteri, seleziona un criterio, quindi uno o più valori per quel criterio.

   b. Continua a creare altri filtri allo stesso modo.

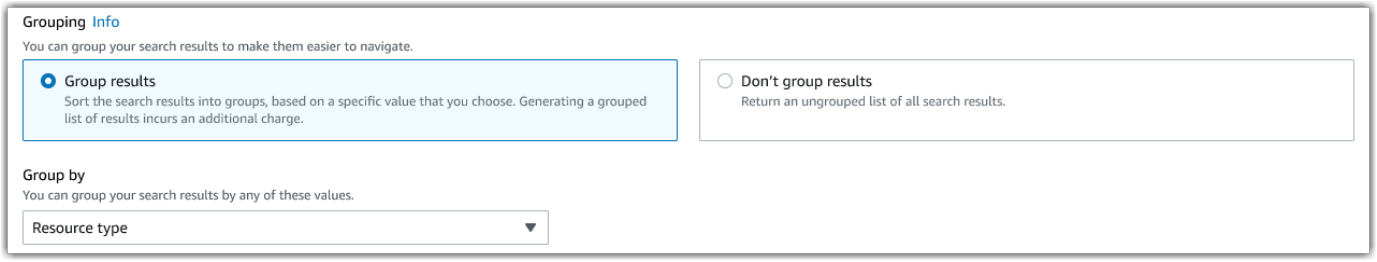
   c. Per rimuovere un filtro indesiderato, scegli Rimuovi.



5. In Raggruppamento, specifica se desideri raggruppare i risultati della ricerca.

   a. Se desideri raggruppare i risultati, seleziona un valore in base al quale raggruppare i risultati.

   b. Se non si desidera raggruppare i risultati, procedi al passaggio 6.



6. Selezionare Search (Cerca).

La ricerca potrebbe richiedere alcuni minuti, a seconda della quantità di dati di prova di cui disponi. Sentiti libero di abbandonare evidence finder mentre la ricerca è in corso. Un avviso lampeggiante ti avvisa quando i risultati della ricerca sono pronti.

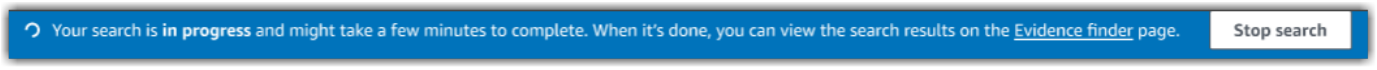
Interruzione di una query di ricerca

Per interrompere una query di ricerca per qualsiasi motivo, attieniti alla seguente procedura.

> **Note**
>
> L'interruzione di una query di ricerca può comunque comportare addebiti. Ti sarà addebitata la quantità di dati delle prove che è stata scansionata prima dell'interruzione della query di ricerca. Una volta interrotta, puoi visualizzare i risultati parziali restituiti.

Interruzione di una query di ricerca in corso

1. Nella barra flash di avanzamento blu nella parte superiore della schermata, seleziona Interrompi la ricerca.



2. (Facoltativo) Esamina i risultati parziali restituiti prima di interrompere la query di ricerca.
   a. Se ti trovi nella pagina evidence finder, i risultati parziali vengono visualizzati sullo schermo.
   b. Se hai abbandonato l'evidence finder, scegli Visualizza risultati parziali nella barra flash di conferma verde.

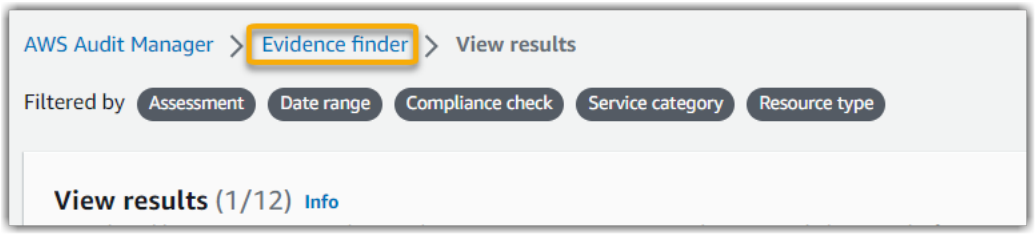
Modifica dei filtri di ricerca

Segui questi passaggi per tornare alla query di ricerca più recente e modificare i filtri secondo necessità.

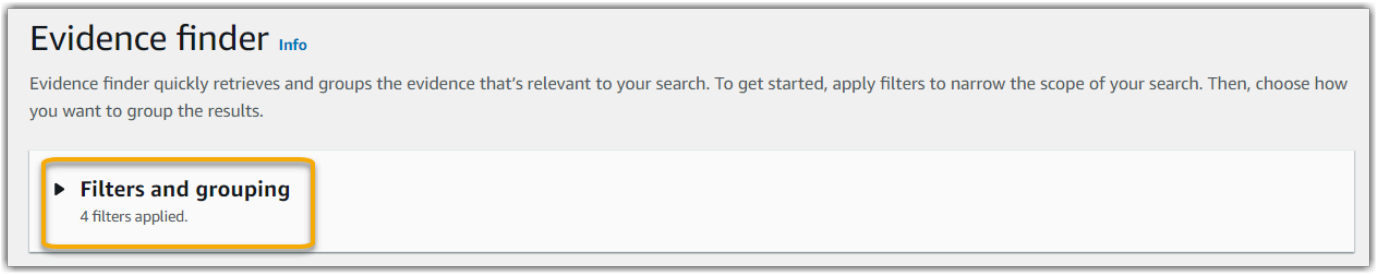
> **Note**
>
> Quando modifichi i filtri e scegli Cerca, viene avviata una nuova query di ricerca.

Modifica di una query di ricerca recente

1. Dalla pagina Visualizza i risultati, scegli Evidence finder dal menu percorso di navigazione.



2. Scegli Filtri e raggruppamento per espandere la selezione dei filtri.



3. Successivamente, modifica i filtri o avvia una nuova ricerca.

   a. Per modificare i filtri, modifica o rimuovi i filtri correnti e la selezione di raggruppamento.

   b. Per ricominciare, scegli Cancella filtri e applica i filtri e la selezione di raggruppamento che preferisci.

4. Al termine, seleziona Cerca.

Passaggi successivi

Al termine della ricerca, puoi visualizzare i risultati che corrispondono ai tuoi criteri di ricerca. Per istruzioni, consulta Visualizzazione dei risultati in evidence finder.

Risorse aggiuntive

- Opzioni di filtro e raggruppamento per Evidence Finder.
- Esempi di casi d'uso per Evidence Finder.
- Risoluzione dei problemi in Evidence Finder.

Visualizzazione dei risultati in evidence finder

Al termine della ricerca, puoi visualizzare i risultati che corrispondono ai tuoi criteri di ricerca.

Durante la raccolta delle prove potrebbero essere valutate più risorse. Di conseguenza, le prove possono includere una o più risorse correlate. In evidence finder, i risultati vengono visualizzati a livello di risorsa, con una riga per ogni risorsa. È possibile visualizzare in anteprima un riepilogo di ogni risorsa senza uscire dalla pagina.

Dopo aver esaminato i risultati della ricerca, puoi generare un rapporto di valutazione che includa tali prove. Puoi anche esportare i risultati della ricerca in un file di valori separati da virgola (CSV).

> **Important**
>
> Ti consigliamo di tenere evidence finder aperto fino al termine dell'esplorazione dei risultati della ricerca. I risultati della ricerca vengono eliminati quando esci dalla tabella Visualizza

risultati. Se necessario, puoi visualizzare i risultati recenti nella CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/. Qui, i risultati delle tue query di ricerca vengono conservati per sette giorni. Tuttavia, tieni presente che non puoi generare un rapporto di valutazione dai risultati di ricerca nella CloudTrail console.

Prerequisiti

La procedura seguente presuppone che tu abbia già seguito i passaggi per eseguire una ricerca in Evidence Finder.

Procedura

Segui questi passaggi per visualizzare i risultati della ricerca in Evidence Finder.

Attività

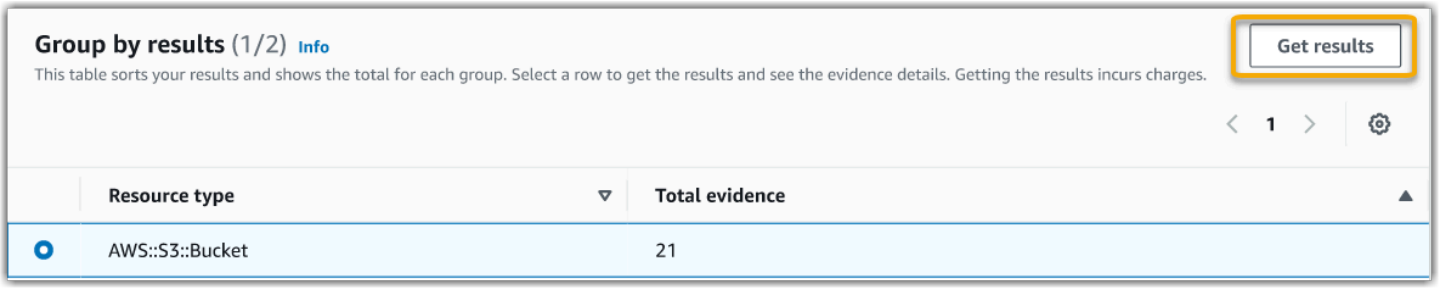
- Fase 1: Visualizzazione dei risultati raggruppati
- Fase 2: Visualizzazione dei risultati
  - Gestione delle preferenze di visualizzazione
  - Visualizzazione in anteprima dei riepiloghi delle risorse

Fase 1: Visualizzazione dei risultati raggruppati

Se hai raggruppato i risultati, puoi rivederli prima di approfondire le prove.

> **Note**
>
> Se non hai raggruppato i risultati, evidence finder non mostra la tabella Raggruppa per risultati. Verrai invece indirizzato direttamente alla tabella Visualizza risultati.

Utilizza la tabella Raggruppa per risultati per conoscere l'ampiezza delle evidenze corrispondenti e come sono distribuite in una dimensione specifica. I risultati vengono raggruppati in base al valore selezionato. Ad esempio, se hai raggruppato per tipo di risorsa, la tabella mostra un elenco di tipi di AWS risorse. La colonna Prova totale mostra il numero di risultati corrispondenti per ogni tipo di risorsa.



Ottenimento dei risultati per un gruppo

1. Dalla tabella Raggruppa per risultati, seleziona la riga relativa ai risultati che desideri ottenere.
2. Scegli Ottieni risultati. Questo avvia una nuova query di ricerca e ti reindirizza alla tabella Visualizza risultati, dove puoi vedere i risultati per quel gruppo.

Fase 2: Visualizzazione dei risultati

La tabella Visualizza risultati mostra i risultati della ricerca. Da qui, puoi gestire le tue preferenze di visualizzazione e visualizzare in anteprima i riepiloghi delle risorse.

Gestione delle preferenze di visualizzazione

Le tue preferenze di visualizzazione controllano ciò che vedi nella pagina dei risultati.

Gestione delle tue preferenze di visualizzazione

1. Scegli l'icona delle impostazioni (#) nella parte superiore della tabella Visualizza risultati.
2. Rivedi e modifica le seguenti impostazioni come necessario:

Impostazione	Descrizione
Seleziona le colonne visibili della tabella	Utilizzate l'opzione di commutazione per modificare le colonne visualizzate.
Dimensioni della pagina	Seleziona un pulsante di opzione per specificare il numero di risultati visualizzati su ogni pagina.
Wrap text (Testo con ritorno a capo)	Seleziona la casella di controllo per disporre lunghe righe di testo per una migliore leggibilità.

3. Per salvare le preferenze, scegli Conferma.

Visualizzazione in anteprima dei riepiloghi delle risorse

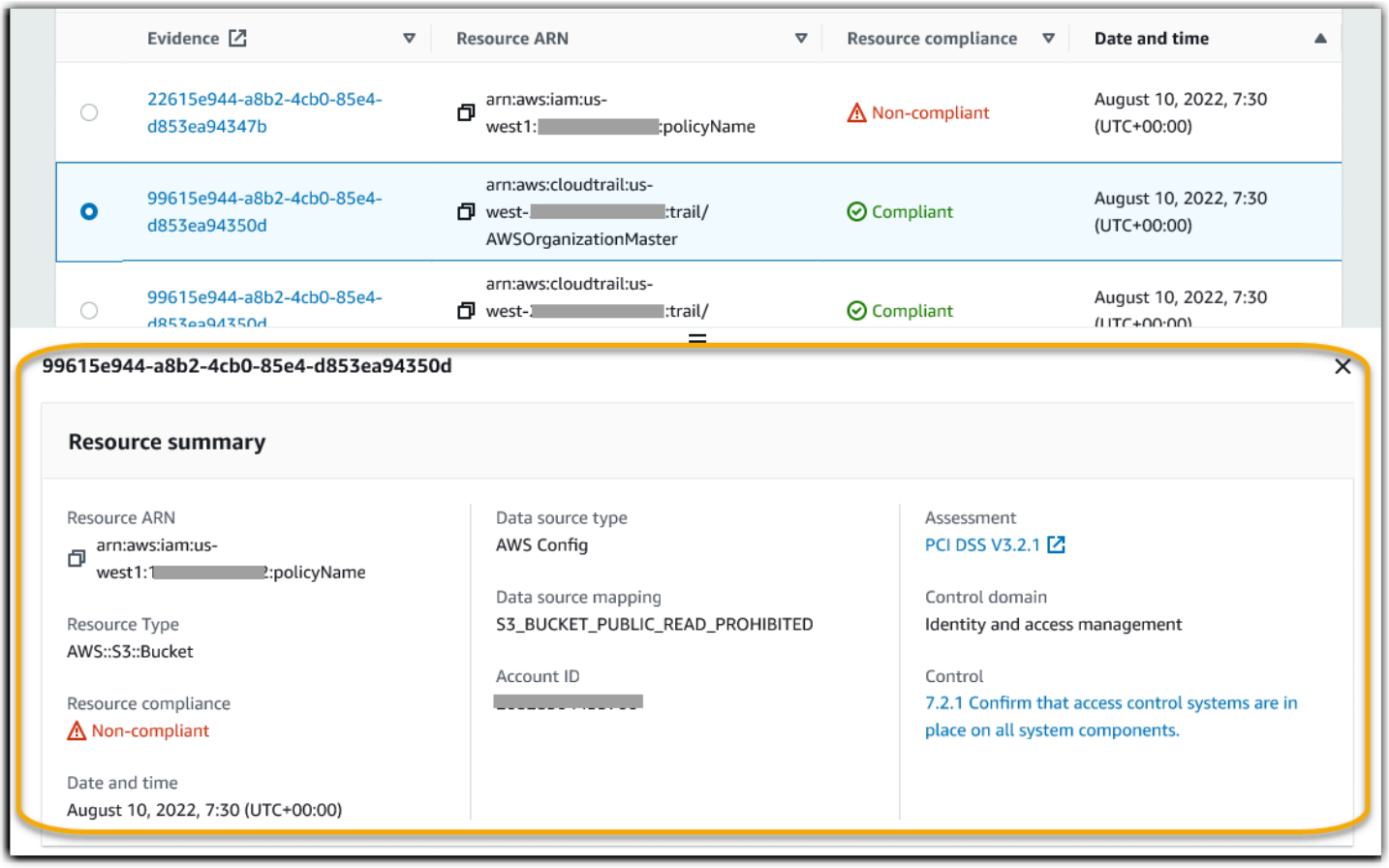
Puoi visualizzare in anteprima le risorse correlate alle prove che corrispondono alla tua query di ricerca. Ciò consente di determinare se la query di ricerca ha restituito i risultati desiderati o se è necessario modificare i filtri ed eseguire nuovamente la query di ricerca.

Tieni presente che le prove possono contenere una o più risorse correlate. Evidence finder mostra i risultati a livello di risorsa (con una riga per ogni risorsa).

> **Note**
>
> Evidence finder restituisce risultati per prove automatiche e manuali. Tuttavia, puoi visualizzare in anteprima solo i riepiloghi delle risorse per prove automatiche. Questo perché Gestione audit non esegue valutazioni delle risorse per prove manuali e, di conseguenza, non è disponibile un riepilogo delle risorse.
> Per visualizzare i dettagli sulle prove manuali, scegli il nome delle prove per aprire la pagina dei dettagli delle prove. Se generi un rapporto di valutazione in base ai risultati del sistema di ricerca delle prove, i dettagli delle prove manuali vengono inclusi nel rapporto di valutazione.

VIsualizzazione dell'anteprima dei riepiloghi delle risorse

1. Seleziona il pulsante di opzione accanto a un risultato. Si apre un pannello di riepilogo delle risorse nella pagina corrente.
2. (Facoltativo) Per visualizzare tutti i dettagli delle prove correlate, scegli il nome della prova.
3. (Facoltativo) Utilizza le linee orizzontali (=) per trascinare e ridimensionare il riquadro di riepilogo delle risorse.
4. Scegli (x) per chiudere il riquadro di riepilogo delle risorse.



Passaggi successivi

Dopo aver esaminato i risultati della ricerca, puoi generare un rapporto di valutazione o esportarli come file CSV. Per istruzioni, consulta Esportazione dei risultati della ricerca da Evidence Finder.

Risorse aggiuntive

- Opzioni di filtro e raggruppamento per Evidence Finder
- Esempi di casi d'uso per Evidence Finder
- Risoluzione dei problemi in Evidence Finder

Esportazione dei risultati della ricerca da Evidence Finder

Dopo aver esaminato i risultati della ricerca, puoi generare un rapporto di valutazione basato su tali risultati. In alternativa, puoi esportare i risultati della ricerca di Evidence Finder in un file CSV.

Prerequisiti

La procedura seguente presuppone che tu abbia già seguito i passaggi per eseguire una ricerca e rivedere i risultati della ricerca in Evidence Finder.

Procedura

Indice

Generazione di un rapporto di valutazione dai risultati della ricerca

Dopo essere soddisfatto dei risultati della ricerca, puoi generare un rapporto di valutazione.

Generazione di un report di valutazione dai risultati della ricerca

1. Nella parte superiore della tabella Visualizza risultati, scegli Genera report di valutazione.
2. Inserisci un nome e una descrizione per il report di valutazione ed esamina i dettagli del report di valutazione.
3. Scegli Genera report di valutazione.

Per generare il report di valutazione saranno necessari alcuni minuti. Mentre ciò accade, puoi uscire da evidence finder e una notifica di successo verde confermerà quando il report è pronto. È quindi possibile accedere al centro download di Gestione audit e scaricare il report di valutazione.

> **Note**
>
> Gestione audit genera un report una tantum utilizzando solo le prove dei risultati della ricerca. Questo report non include alcuna prova aggiunta manualmente a un report dalla pagina di valutazione.
> Si applicano dei limiti alla quantità di prove che possono essere incluse in un report di valutazione. Per ulteriori informazioni, consulta Risoluzione dei problemi in Evidence Finder.

Esportazione dei risultati della ricerca in un file CSV

Potresti aver bisogno di una versione portatile dei risultati di ricerca del tuo evidence finder. In tal caso, puoi esportare i risultati della ricerca in un file CSV.

Dopo aver esportato i risultati della ricerca, il file CSV è disponibile nel centro download Gestione audit per sette giorni. Una copia del file CSV viene inoltre consegnata al bucket S3 preferito, noto come destinazione di esportazione. Il file CSV rimane disponibile in questo bucket finché non lo elimini.

Audit Manager utilizza la funzionalità CloudTrail Lake per esportare e fornire file CSV da Evidence Finder. I seguenti fattori definiscono il funzionamento del processo di esportazione in formato CSV:

- Tutti i risultati della ricerca sono inclusi nel file CSV. Se desideri includere solo risultati di ricerca specifici, ti consigliamo di modificare i filtri di ricerca. In questo modo, puoi restringere i risultati in modo da indirizzare solo le prove che desideri esportare.
- I file CSV vengono esportati in formato GZIP compresso. Il nome del file CSV predefinito è `queryID/result.csv.gz`, dove `queryID` è l'ID della query di ricerca.
- Le dimensioni file massime per un'esportazione in formato CSV sono di 1 TB. Se esporti più di 1 TB di dati, i risultati vengono suddivisi in più di un file. Ogni file CSV è denominato `result_`*`number`*`.csv.gz`. Il numero di file CSV che ottieni dipende dalla dimensione totale dei risultati della ricerca. Ad esempio, l'esportazione di 2 TB di dati fornisce due file di risultati delle query: `result_1.csv.gz` e `result_2.csv.gz`.
- Oltre al file CSV, nel bucket S3 viene inviato un file di firma JSON. Questo file funge da checksum per verificare che le informazioni all'interno del file CSV siano accurate. Per ulteriori informazioni, consulta la struttura CloudTrail dei file di firma nella Guida per gli AWS CloudTrail sviluppatori. Per determinare se i risultati della query sono stati modificati, eliminati o sono rimasti invariati dopo la consegna, è possibile utilizzare la convalida dell'integrità dei risultati delle CloudTrail query. Per istruzioni, vedi Convalidare i risultati delle query salvate nella Guida per gli sviluppatori AWS CloudTrail .

> **Note**
>
> Le risposte testuali manuali alle prove non sono attualmente incluse nelle anteprime di evidence finder o nelle esportazioni in formato CSV. Per visualizzare i dati delle risposte testuali, scegli il nome delle prove manuali nei risultati di Evidence finder per aprire la pagina dei dettagli delle prove. Se è necessario visualizzare i dati di risposta testuale al di fuori

della console Gestione audit, si consiglia di generare un rapporto di valutazione dai risultati dell'evidence finder. Tutti i dettagli manuali sulle prove, comprese le risposte testuali, sono inclusi nei report di valutazione.

Esportazione dei risultati per la prima volta

Segui questa procedura per esportare i risultati della ricerca per la prima volta. Questa procedura offre la possibilità di specificare una destinazione di esportazione predefinita per tutte le esportazioni future. Se non desideri salvare subito una destinazione di esportazione predefinita, puoi farlo in un secondo momento aggiornando le impostazioni della destinazione di esportazione.

Important

Prima di iniziare, assicurati di avere a disposizione un bucket S3 da utilizzare come destinazione di esportazione. Puoi usare uno dei tuoi bucket S3 esistenti oppure puoi creare un nuovo bucket in Amazon S3. Inoltre, il bucket S3 deve disporre della politica di autorizzazioni necessaria per consentire la scrittura dei file di esportazione CloudTrail al suo interno. Più specificamente, la policy del bucket deve includere un'`s3:PutObject`azione e l'ARN del bucket ed essere elencata CloudTrail come principale del servizio. Forniamo un esempio di policy di autorizzazione che puoi utilizzare. Per istruzioni su come collegare questa policy al tuo bucket S3, vedi Aggiungere una policy del bucket utilizzando la console Amazon S3.
Per ulteriori suggerimenti, consulta. Suggerimenti di configurazione per la destinazione di esportazione Se riscontri problemi durante l'esportazione di un file CSV, consulta. csv-exports

Esportazione dei risultati della ricerca (esperienza di prima esecuzione)

1. Nella parte superiore della tabella Visualizza risultati, scegli Esporta CSV.
2. Specifica il bucket S3 in cui desideri esportare i file.
   - Scegli Sfoglia S3 per selezionarlo dall'elenco dei bucket.
   - In alternativa, puoi inserire l'URI del bucket in questo formato: **`s3://bucketname/prefix`**

> **Tip**
>
> Per mantenere organizzato il bucket di destinazione, puoi creare una cartella opzionale per le esportazioni in formato CSV. A tale scopo, aggiungi una barra (**/**) e un prefisso al valore nella casella URI di risorsa (ad esempio, **/evidenceFinderExports**). Gestione audit include quindi questo prefisso quando aggiunge il file CSV al bucket e Amazon S3 genera il percorso specificato dal prefisso. Per ulteriori informazioni sui prefissi in Amazon S3, vedi Organizzare oggetti nella console Amazon S3 nella Guida per l'utente Amazon Simple Storage Service.

3. (Facoltativo) Se non desideri salvare questo bucket come destinazione di esportazione predefinita, deseleziona la casella di controllo Salva questo bucket come destinazione di esportazione predefinita nelle impostazioni del mio evidence finder.
4. Scegli Export (Esporta).

Esportazione dei risultati dopo aver salvato una destinazione di esportazione

Dopo aver salvato un bucket S3 predefinito come destinazione di esportazione predefinita, puoi seguire questi passaggi da ora in avanti.

Esportazione dei risultati della ricerca (dopo aver salvato una destinazione di esportazione predefinita)

1. Nella parte superiore della tabella Visualizza risultati, scegli Esporta CSV.
2. Nel prompt che appare, controlla il bucket S3 predefinito in cui verrà salvato il file esportato.
   a. (Facoltativo) Per continuare a utilizzare questo bucket e nascondere questo messaggio in futuro, seleziona la casella Non ricordarmelo più.
   b. (Facoltativo) Per modificare questo bucket, segui la procedura per aggiornare le impostazioni della destinazione di esportazione.
3. Scegli Conferma.

A seconda della quantità di dati che stai esportando, il completamento del processo di esportazione può richiedere alcuni minuti. Puoi uscire da evidence finder mentre l'esportazione è in corso. Quando esci da evidence finder, la ricerca viene interrotta e i risultati della ricerca vengono eliminati nella

console. Tuttavia, il processo di esportazione in formato CSV continua sullo sfondo. Il file CSV conterrà il set completo di risultati di ricerca corrispondenti alla tua query.

Visualizzazione dei risultati dopo averli esportati

Per trovare il tuo file CSV e verificarne lo stato, vai all'Audit ManagerCentro di download di Gestione audit. Quando il file esportato è pronto, puoi scaricare il file CSV dal centro download.

Puoi anche trovare e scaricare il file CSV dal bucket S3 di destinazione dell'esportazione.

Ritrovamento del file CSV e del file di firma nella console Amazon S3

1. Apri la console Amazon S3.
2. Scegli il bucket di destinazione di esportazione che hai specificato quando hai esportato il file CSV.
3. Esplora la gerarchia di oggetti fino a trovare il file CSV e di firma desiderati. Il file CSV ha un'estensione `.csv.gz` e il file di firma ha un'estensione `.json`.

Sarà possibile navigare in una gerarchia di oggetti simile a quella dell'esempio seguente, ma con valori diversi per nome di bucket della destinazione di esportazione, ID account, regione e data.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Risorse aggiuntive

- Risoluzione dei problemi in Evidence Finder
- Configurazione della destinazione di esportazione predefinita per Evidence Finder

Opzioni di filtro e raggruppamento per Evidence Finder

In questa pagina, puoi visualizzare un elenco delle opzioni di filtro e raggruppamento disponibili per l'utilizzo in Evidence Finder.

Riferimento al filtro

Puoi utilizzare i seguenti filtri per trovare prove che soddisfano criteri specifici, come una valutazione, un controllo o. Servizio AWS

Argomenti

Filtri obbligatori

Utilizza questi filtri per iniziare con una panoramica di alto livello delle prove di una valutazione.

Nome del filtro	Descrizione	Note
Valutazione	Restituisce le prove per una valutazione specifica.	Puoi filtrare in base a una sola valutazione.
Intervallo di date	Restituisce le prove per un determinato periodo di tempo.	In entrambi i casi, è possibile utilizzare un intervallo relativo per definire un intervallo relativo alla data odierna (ad esempio, **`Last 30 days`**). In alternativa, puoi utilizzare un intervallo assoluto per specificare un intervallo di date specifico (ad esempio, **`June 27th - July 4th`**).
Conformità delle risorse	Restituisce risorse con una valutazione specifica del controllo di conformità.	Audit Manager raccoglie prove di verifica della conformità per i controlli che utilizzano AWS Config Security Hub come tipo di origine dati. Durante la raccolta delle prove potrebbero essere valutate più risorse. Di conseguenza, una singola prova di controllo di conformità può includere una o

Nome del filtro	Descrizione	Note
		più risorse. È possibile utilizzare questo filtro per esaminare lo stato di conformità a livello di risorsa. Puoi scegliere una delle seguenti opzioni: • Non conforme: questo filtro trova risorse con problemi di controllo della conformità. Ciò accade se Security Hub riporta un risultato Fail o se AWS Config riporta un risultato non conforme. • Conforme: questo filtro trova risorse che non hanno problemi di controllo della conformità. Ciò accade se Security Hub riporta un risultato Pass o se AWS Config riporta un risultato conforme. • Inconcludente: questo filtro trova le risorse per le quali un controllo di conformità non è disponibi le o applicabile. Ciò accade se una risorsa usa AWS Config o Security Hub come tipo di origine dati sottostante, ma tali servizi non sono abilitati . Ciò accade anche se la risorsa utilizza un tipo di origine dati sottostante che non supporta i controlli di conformità (come prove manuali, chiamate AWS API o CloudTrail).

Filtri aggiuntivi (facoltativi)

Utilizza questi filtri per restringere l'ambito della tua query di ricerca. Ad esempio, usa Servizio per visualizzare tutte le prove relative ad Amazon S3. Usa Tipo di risorsa per concentrarti solo sui bucket S3. Oppure, usa ARN della risorsa per indirizzare un bucket S3 specifico.

È possibile creare filtri aggiuntivi utilizzando uno o più dei seguenti criteri.

Nome del criterio	Descrizione	Quando utilizzare questi criteri
ID account	Approfondisci per Account AWS.	Usa questi criteri per trovare prove correlate a uno specifico Account AWS.
Controllo	Esamina il dettaglio in base al nome del controllo.	Usa questi criteri per trovare prove correlate a uno specifico controllo.
Dominio di controllo	Analizza in base al dominio di controllo.	Utilizza questi criteri per concentrarti su un'area tematica specifica mentre ti prepari per un audit. Puoi filtrare per dominio di controllo se stai interrogando una valutazione creata da un framework standard. Esempi di domini di controllo includono la gestione delle identità e degli accessi, la registrazione e il monitoraggio e la gestione della rete.
Data source type (Tipo di origine dati)	Analizza in base al tipo di origine dati.	Usa questi criteri per concentrarti su una fonte di dati specifica. Imposta il valore su `Manual` per trovare le prove che hai caricato manualmente. Altrimenti, puoi filtrare le prove automatizzate in base alla loro provenienza (ad esempio `AWS Config`, `CloudTrail` , `Security Hub`, o `AWS API calls`).
Nome evento	Analizza in base al nome dell'evento.	Usa questi criteri per concentrarti su un evento specifico a cui sono correlate le prove. Un evento in corrisponde al record di un'attività in un Account AWS. Ad esempio, puoi cercare il nome di una chiamata API, ad esempio l'operazione `AttachRolePolicy` IAM utilizzata per configurare le autorizzazioni. Oppure, cerca una CloudTrail parola chiave, ad esempio l'`ConsoleLo`

Nome del criterio	Descrizione	Quando utilizzare questi criteri
		`gin` evento registrato CloudTrail quando un utente accede al tuo account.
ARN risorsa	Analizza in base al Nome della risorsa Amazon (ARN - Amazon Resource Name).	Utilizza questi criteri per trovare prove correlate a una risorsa specifica AWS .
Tipo di risorsa	Approfondisci per tipo di risorsa.	Utilizza questi criteri per concentrarti sul tipo di risorsa da valutare, ad esempio un'istanza Amazon EC2 o un bucket S3.
Servizio	Approfondisci per nome. Servizio AWS	Utilizza questi criteri per trovare prove correlate a uno specifico Servizio AWS, come Amazon EC2, Amazon S3 o. AWS Config
Categoria di servizio	Approfondisci per categoria. Servizio AWS	Utilizza questi criteri per concentrarti su una categoria specifica di Servizio AWS. Gli esempi includono sicurezza, identità e conformità, database e archiviazione.

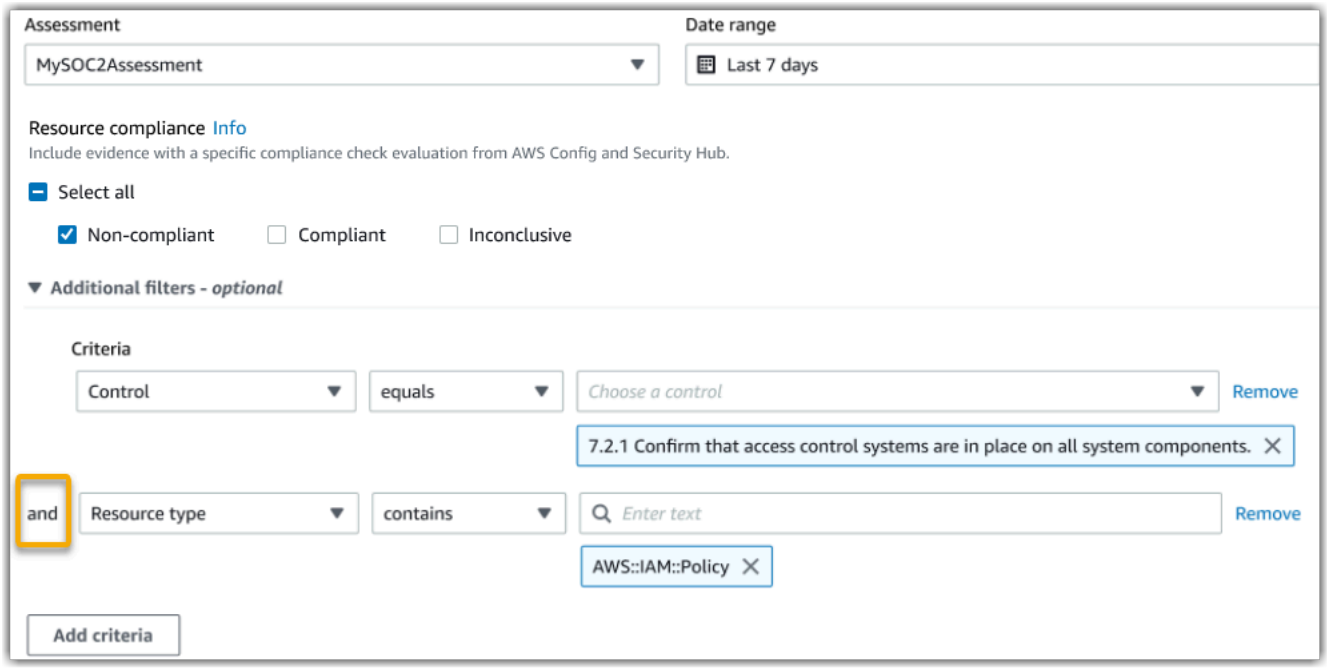
Combinazione di filtri

Comportamento dei criteri

Quando si specifica più di un criterio, Gestione audit applica l'operatore `AND` alle selezioni. Ciò significa che tutti i criteri sono raggruppati in un'unica query e i risultati devono corrispondere a tutti i criteri combinati.

Esempio

Nella seguente configurazione del filtro, evidence finder restituisce le risorse non conformi degli ultimi 7 giorni per la valutazione richiesta **`MySOC2Assessment`**. Inoltre, i risultati si riferiscono sia a una policy IAM che al controllo specificato.

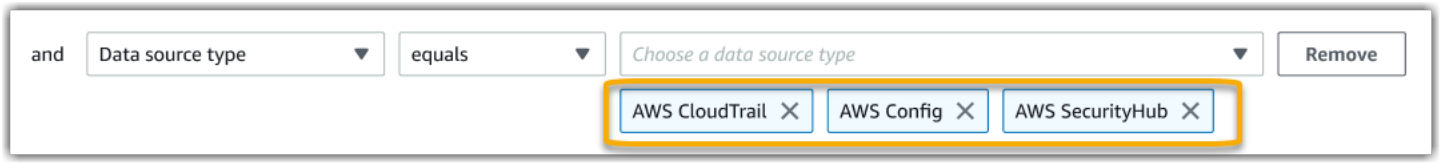


Comportamento del valore criteri

Quando si specifica più di un valore di criterio, i valori vengono collegati a un operatore `OR`. evidence finder restituisce risultati che corrispondono a uno qualsiasi di questi valori dei criteri.

Esempio

Nella seguente configurazione del filtro, Evidence Finder restituisce i risultati di ricerca provenienti da AWS CloudTrail, AWS Config, o AWS Security Hub.



Riferimento di raggruppamento

Puoi raggruppare i risultati della ricerca per una navigazione più rapida. Il raggruppamento mostra l'ampiezza dei risultati di ricerca e come sono distribuiti in una dimensione specifica.

È possibile utilizzare uno dei seguenti gruppi per valori.

Gruppo da	Descrizione
ID account	Raggruppa i risultati per Account AWS.
Controllo	Raggruppa i risultati per nome del controllo.
Data source type (Tipo di origine dati)	Raggruppa i risultati in base al tipo di origine dati da cui provengono le prove.
Nome evento	Raggruppa i risultati in base al nome dell'evento.
ARN risorsa	Raggruppa i risultati per Nome della risorsa Amazon (ARN).
Tipo di risorsa	Raggruppa i risultati per tipo di risorsa.
Servizio	Raggruppa i risultati per Servizio AWS nome.
Categoria di servizio	Raggruppa i risultati per Servizio AWS categoria.

Esempi di casi d'uso per Evidence Finder

Evidence finder può aiutarti in diversi casi d'uso. Questa pagina fornisce alcuni esempi e suggerisce i filtri di ricerca che è possibile utilizzare in ogni scenario.

Argomenti

Caso d'uso 1: trovare prove non conformi e organizzare le delegazioni

Questo caso d'uso è ideale se sei un responsabile della conformità, un responsabile della protezione dei dati o un professionista GRC che supervisiona la preparazione degli audit.

Mentre monitori il livello di conformità della tua organizzazione, potresti affidarti a team di partner per aiutarti a risolvere i problemi. Puoi utilizzare evidence finder per aiutarti a organizzare il lavoro per i team dei tuoi partner.

Applicando i filtri, puoi concentrarti sulle prove relative a un'area alla volta. Inoltre, puoi anche rimanere in linea con le responsabilità e l'ambito di ogni team partner con cui lavori. Eseguendo una ricerca mirata in questo modo, puoi utilizzare i risultati della ricerca per identificare esattamente ciò che deve essere corretto in ciascuna area tematica. È quindi possibile delegare tali prove non conformi al team partner corrispondente per la correzione.

Per questo flusso di lavoro, segui i passaggi per cercare prove. Utilizza i seguenti filtri per trovare prove non conformi.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Successivamente, applica filtri aggiuntivi per l'area su cui ti stai concentrando. Ad esempio, utilizza il filtro Categoria di servizio per trovare risorse non conformi correlate a IAM. Quindi, condividi questi risultati con il team che possiede le risorse IAM per la tua organizzazione. Oppure, se stai interrogando una valutazione creata da un framework standard, puoi utilizzare il filtro Dominio di controllo per trovare prove non conformi correlate al dominio di gestione delle identità e degli accessi.

```
Control domain | <domain that you're focusing on>
or
Service category | <Servizio AWS category that you're focusing on>
```

Dopo aver trovato le prove di cui hai bisogno, segui i passaggi per generare un rapporto di valutazione dai risultati della ricerca. Per istruzioni, consulta Generazione di un rapporto di valutazione dai risultati della ricerca. Puoi condividere questo rapporto con il tuo team partner, che può utilizzarlo come lista di controllo per la correzione.

Caso d'uso 2: Identifica le prove conformi

Questo caso d'uso è ideale se lavori nel settore SecOps IT/ DevOps o in un altro ruolo che possiede e ripara risorse cloud.

Nell'ambito di un audit, è possibile che ti venga chiesto di risolvere i problemi relativi alle risorse di cui sei proprietario. Dopo aver svolto questo lavoro, puoi utilizzare evidence finder per verificare che le tue risorse siano conformi.

Per questo flusso di lavoro, segui i passaggi per cercare prove. Utilizza i seguenti filtri per trovare prove conformi.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Successivamente, applica filtri aggiuntivi per mostrare solo le prove di cui sei responsabile. A seconda dell'ambito di proprietà, rendi la ricerca mirata in base alle esigenze. I seguenti esempi di filtri sono ordinati dal più ampio al più preciso. Scegli le opzioni appropriate per te e sostituisci il *<testo segnaposto>* con i tuoi valori.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Servizi AWS that you own>
Service | <a specific Servizio AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

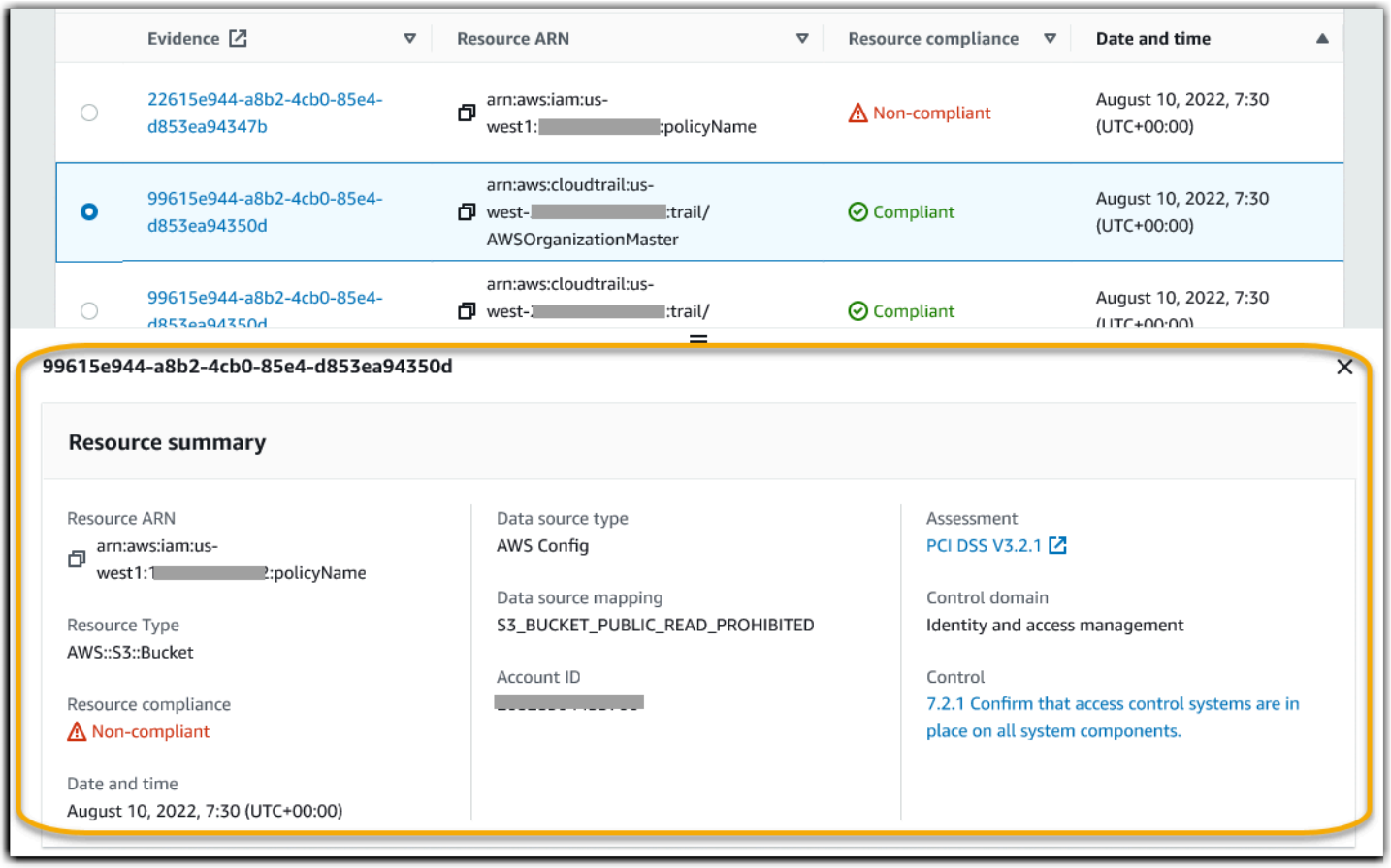
Se sei responsabile di più istanze con gli stessi criteri (ad esempio, ne possiedi più Servizi AWS), puoi raggruppare i risultati in base a quel valore. Ciò ti fornisce le evidenze totali corrispondenti per ciascun Servizio AWS. È quindi possibile ottenere i risultati per i servizi di cui sei proprietario.

Caso d'uso 3: Esegui una rapida anteprima delle risorse relative alle prove

Questo caso d'uso è ideale per tutti i clienti Gestione audit.

In precedenza, esamina i dettagli delle singole prove richiedeva molto tempo. Se volevi visualizzare in anteprima le prove, dovevi passare direttamente a quella valutazione, quindi sfogliare cartelle di prove ben raggruppate. Ora, evidence finder offre un modo pratico per visualizzare queste informazioni in anteprima. Per ogni elemento di prova che corrisponde alla tua query di ricerca, puoi visualizzare in anteprima le singole risorse relative a tale prova.

Per iniziare, segui i passaggi per cercare prove. Quindi seleziona il pulsante di opzione accanto a un risultato per visualizzare un riepilogo della risorsa nella pagina corrente. Puoi visualizzare in anteprima ogni singola risorsa relativa a un elemento di prova. Per visualizzare i dettagli completi delle prove per qualsiasi risorsa, scegli il nome della prova. Per ulteriori informazioni, consulta Visualizzazione in anteprima dei riepiloghi delle risorse.


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Centro di download di Gestione audit

Il centro di download è dove puoi trovare e gestire tutti i tuoi file di Gestione audit scaricabili. Quando generi un report di valutazione o esporti i risultati della ricerca da Evidence Finder, i file vengono visualizzati nel centro di download.

Indice

Navigazione nel centro di download

Segui questi passaggi per sfogliare i file nel centro download.

Per trovare i file nel centro download

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Centro di download.
3. Scegli la scheda Rapporti di valutazione per visualizzare i rapporti di valutazione disponibili per il download.

    - Questa scheda mostra i rapporti di valutazione che hai generato. I report di valutazione rimangono disponibili nel centro di download fino a quando non vengono eliminati.
    - Per visualizzare lo stato più recente del tuo report di valutazione, scegli l'icona di aggiornamento (#) per ricaricare la tabella. Ogni riga della tabella dei report di valutazione mostra il nome del report, la data di creazione e uno dei seguenti stati:

Stato	Descrizione
In corso	Audit Manager sta generando il rapporto di valutazione.
Pronto	Il rapporto di valutazione può essere scaricato.

Stato	Descrizione
Errore	Il rapporto di valutazione non è stato generato. In questo caso, Gestione audit visualizza un messaggio che descrive l'errore. Per informazioni su come risolvere questi errori, vedereRisoluzione dei problemi relativi ai report di valutazione.

4. Scegli la scheda Esportazioni per visualizzare le esportazioni CSV disponibili per il download.

   - Questa scheda mostra i risultati della ricerca di Evidence Finder che hai esportato negli ultimi sette giorni. I file CSV vengono rimossi dal centro di download dopo sette giorni, ma rimangono disponibili nel bucket S3 destinazione dell'esportazione. Per istruzioni su come trovare un'esportazione in formato CSV di Evidence Finder nel tuo bucket di destinazione S3, consulta Visualizzazione dei risultati dopo averli esportati.
   - Per visualizzare lo stato più recente delle tue esportazioni in formato CVS, scegli l'icona di aggiornamento (#) per ricaricare la tabella. Ogni riga della tabella delle esportazioni mostra il nome del file, la data di esportazione e uno dei seguenti stati:

Stato	Descrizione
In corso	Audit Manager sta preparando il file CSV.
Pronto	L'esportazione è riuscita e il file è disponibile per il download.
Errore	L'esportazione non è riuscita. In questo caso, Gestione audit visualizza un messaggio che descrive l'errore. Per informazioni su come risolvere questi errori, vederecsv-exports.

> **Note**
>
> Tieni presente che la scheda delle esportazioni potrebbe mostrare anche file CSV per le query che hai eseguito direttamente in AWS CloudTrail Lake. Ciò include le query effettuate nella CloudTrail console o utilizzando l'API. CloudTrail CloudTrail le

esportazioni vengono visualizzate in questa scheda se hai interrogato l'archivio dati degli eventi Audit Manager e hai scelto di salvare i risultati su Amazon S3.

Scaricamento di un file

Segui questi passaggi per scaricare un file dal centro di download.

Per scaricare un file

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Centro di download.
3. Scegli la scheda Report di valutazione o la scheda Esportazioni.
4. Seleziona il file che desideri scaricare, quindi scegli Scarica.

Per istruzioni su come scaricare un file direttamente dal tuo bucket di destinazione S3, consulta Downloading an object nella Amazon Simple Storage Service (Amazon S3) User Guide.

Eliminazione di un file

Segui questi passaggi per eliminare tutti i report di valutazione che non ti servono più nel centro di download.

> **Note**
>
> L'eliminazione di esportazioni in formato CSV dal centro di download non è attualmente supportata. Le esportazioni in formato CSV vengono rimosse automaticamente dal centro di download dopo sette giorni.

Per eliminare un report di valutazione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Centro di download.
3. Scegli la scheda Report di valutazione.

4. Seleziona il report di valutazione che desideri eliminare e scegli Elimina.

Se desideri eliminare un report di valutazione o un'esportazione CSV dal tuo bucket di destinazione S3, ti consigliamo di eseguire questa attività direttamente in Amazon S3. Per istruzioni, consulta Eliminazione di oggetti Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service (Amazon S3).

Risorse aggiuntive

- Configurazione della destinazione di esportazione predefinita per Evidence Finder
- Configurazione della destinazione predefinita del rapporto di valutazione
- Risoluzione dei problemi relativi ai report di valutazione
- Risoluzione dei problemi di esportazione in formato CSV
- Scaricamento di un oggetto da Amazon S3
- Eliminazione di oggetti Amazon S3

Utilizzo della libreria di framework per gestire i framework in AWS Audit Manager

È possibile trovare e gestire i framework nella libreria di framework in. AWS Audit Manager

Un framework determina quali controlli vengono testati in un ambiente per un periodo di tempo. Definisce i controlli e le relative mappature delle origini dati per un determinato standard o regolamento di conformità. Viene inoltre utilizzato per strutturare e automatizzare le valutazioni Gestione audit. È possibile utilizzare i framework come punto di partenza per verificare l' Servizio AWS utilizzo e iniziare ad automatizzare la raccolta delle prove.

Punti chiave

Nella libreria framework, i framework sono organizzati nelle seguenti categorie.

- I framework standard sono framework predefiniti forniti da AWS . Questi framework si basano sulle AWS migliori pratiche per diversi standard e regolamenti di conformità, come GDPR e HIPAA. I framework standard includono controlli organizzati in set di controllo basati sullo standard o sulla regolamentazione di conformità supportati dal framework.

  Puoi visualizzare il contenuto dei framework standard, ma non modificarli o eliminarli. Tuttavia, è possibile creare una copia modificabile di qualsiasi framework standard per crearne uno nuovo che soddisfi requisiti specifici.
- I framework personalizzati sono framework creati dall'utente. È possibile creare un framework personalizzato partendo da zero o creando una copia modificabile di un framework esistente. Puoi utilizzare framework personalizzati per organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici.

Puoi creare una valutazione da un framework standard o da un framework personalizzato.

> **Note**
>
> AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e regolamenti di conformità. Tuttavia, non viene eseguita la valutazione della conformità. AWS Audit Manager Pertanto, le prove raccolte potrebbero non includere tutte le

informazioni sull' AWS utilizzo necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Risorse aggiuntive

Per creare e gestire framework in Audit Manager, segui le procedure descritte qui.

- Individuazione dei framework disponibili in AWS Audit Manager
- Revisione di un framework in AWS Audit Manager
- Creazione di un framework personalizzato in AWS Audit Manager
  - Creare un framework personalizzato partendo da zero in AWS Audit Manager
  - Creazione di una copia modificabile di un framework esistente in AWS Audit Manager
- Modifica di un framework personalizzato in AWS Audit Manager
- Eliminazione di un framework personalizzato in AWS Audit Manager
- Condivisione di un framework personalizzato in AWS Audit Manager
  - Concetti e terminologia di condivisione dei framework
  - Invio di una richiesta di condivisione di un framework personalizzato in AWS Audit Manager
  - Rispondere alle richieste di condivisione in AWS Audit Manager
  - Eliminazione delle richieste di condivisione in AWS Audit Manager
- Framework supportati in AWS Audit Manager

Individuazione dei framework disponibili in AWS Audit Manager

Puoi trovare tutti i framework disponibili nella pagina della libreria Framework nella console Audit Manager.

È inoltre possibile visualizzare tutti i framework disponibili utilizzando l'API Audit Manager o AWS Command Line Interface ()AWS CLI.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i framework. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono e.

AWSAuditManagerAdministratorAccessConsentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Audit Manager console

Per visualizzare i framework disponibili sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Libreria Framework.
3. Scegli la scheda Framework standard o la scheda Framework personalizzati per sfogliare i framework standard e personalizzati disponibili.

AWS CLI

Per visualizzare i framework disponibili nella AWS CLI

Per visualizzare i framework in Audit Manager, utilizzare il list-assessment-frameworkscomando e specificare a. `--framework-type` In entrambi i casi, puoi recuperare un elenco di framework standard. In alternativa, puoi recuperare un elenco di framework personalizzati.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Per visualizzare i framework disponibili utilizzando l'API

Usa l'ListAssessmentFrameworksoperazione e specifica un FrameworkType. In entrambi i casi, puoi restituire un elenco di framework standard. In alternativa, puoi restituire un elenco di framework personalizzati.

Per ulteriori informazioni, scegli uno dei link precedenti per saperne di più nel Riferimento API AWS Audit Manager . Ciò include informazioni su come utilizzare l'`ListAssessmentFrameworks`operazione e i parametri in uno degli SDK specifici della lingua. AWS

Passaggi successivi

Quando sei pronto per esplorare i dettagli di un framework, segui i passaggi indicati. Revisione di un framework in AWS Audit Manager Questa pagina ti guiderà attraverso i dettagli del framework e spiegherà le informazioni in esso contenute.

Dalla pagina della libreria del framework, puoi anche creare, modificare, eliminare o condividere un framework personalizzato.

Risorse aggiuntive

Per le soluzioni ai problemi del framework in Audit Manager, vedereRisoluzione dei problemi relativi al framework.

Revisione di un framework in AWS Audit Manager

Puoi esaminare i dettagli di un framework utilizzando la console Gestione audit, l'API Gestione audit o AWS Command Line Interface (AWS CLI).

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i framework. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono e. AWSAuditManagerAdministratorAccessConsentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Audit Manager console

Per visualizzare i dettagli del framework sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione a sinistra, scegli Libreria Framework per visualizzare un elenco dei framework disponibili.
3. Scegli la scheda Framework standard o la scheda Framework personalizzati per sfogliare i framework disponibili.

4. Scegli il nome del framework per aprirlo.
5. Rivedi i dettagli del framework utilizzando le seguenti informazioni come riferimento.

Sezione dei dettagli del framework

In questa sezione viene fornita una panoramica di ogni framework. In questa sezione, puoi esaminare le seguenti informazioni:

Nome	Description
Descrizione	Una descrizione del framework, se ne è stata fornita una.
Tipo di framework	Speciifica se il framework è un framework standard o un framework personalizzato.
Tipo di conformità	Lo standard o il regolamento di conformità supportato dal framework.

Se stai visualizzando un framework personalizzato, puoi anche visualizzare i seguenti dettagli:

Nome	Descrizione
Creato da	L'account che ha creato il framework personalizzato.
Date created (Data di creazione)	La data in cui è stato creato il framework personalizzato.
Ultimo aggiornamento	La data dell'ultima modifica di questo framework.

Scheda Controlli

Questa scheda elenca i controlli del framework, raggruppati per set di controlli. In questa scheda è possibile esaminare le seguenti informazioni:

Nome	Descrizione
Controlli raggruppati per set di controlli	Scegliete l'icona della visualizzazione ad albero per visualizz are i controlli che appartengono a ciascun set di controlli.
Type	Speciifica se il controllo è un controllo standard o un controllo personalizzato.
Fonti di dati	Speciifica l'origine dei dati da cui Audit Manager raccoglie le prove per quel controllo del framework.

Scheda Tag

Questa scheda elenca i tag associati al framework. In questa scheda, puoi rivedere le seguenti informazioni:

Nome	Descrizione
Chiave	La chiave del tag (ad esempio, uno standard di conformità, un regolamento o una categoria).
Valore	Il valore del tag.

AWS CLI

Per visualizzare i dettagli del framework in AWS CLI

1. Per identificare il framework che desideri esaminare, esegui il list-assessment-frameworkscomando e specifica a`--framework-type`. In entrambi i casi, puoi recuperare un elenco di framework standard. In alternativa, puoi recuperare un elenco di framework personalizzati.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con `Custom` o `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

La risposta restituisce un elenco di framework. Trova il framework che desideri esaminare e prendi nota dell'ID del framework e nome della risorsa Amazon (ARN).

2. Per ottenere i dettagli del framework, esegui il get-assessment-frameworkcomando e specifica`--framework-id`.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   > **Tip**
   >
   > I dettagli del framework vengono restituiti in formato JSON. Per comprendere questi dati, consulta get-assessment-framework Output nel AWS CLI Command Reference.

3. Per vedere i tag di un framework, usa il list-tags-for-resourcecomando e specifica il `--resource-arn` per il framework.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Per ulteriori informazioni sull'utilizzo dei tag in Gestione audit, consulta le risorse Tagging AWS Audit Manager.

Audit Manager API

Per visualizzare i dettagli del framework utilizzando l'API

1. Per identificare il framework che desideri esaminare, utilizza l'ListAssessmentFrameworksoperazione e specifica un FrameworkType. In entrambi i casi, puoi restituire un elenco di framework standard. In alternativa, puoi restituire un elenco di framework personalizzati.

   Dalla risposta, trova il framework che desideri esaminare e prendi nota dell'ID del framework e nome della risorsa Amazon (ARN).

2. Per ottenere i dettagli del framework, utilizzate l'operazione. GetAssessmentFramework Nella richiesta, specifica il frameworkId ottenuto dal passaggio 1.

   > **Tip**
   >
   > I dettagli del framework vengono restituiti in formato JSON. Per comprendere questi dati, consulta GetAssessmentFramework Response Elements nell'AWS Audit Manager API Reference.

3. Per vedere i tag del framework, usa l'ListTagsForResourceoperazione. Nella richiesta, specifica il framework resourceArn ottenuto dal passaggio 1.

Per ulteriori informazioni sui tag in Audit Manager, vedere Tagging AWS Audit Manager resources.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nella Guida di riferimento alle AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Dalla pagina dei dettagli del framework, puoi creare una valutazione dal framework o creare una copia modificabile del framework.

Se stai esaminando un framework personalizzato, puoi anche modificare, eliminare o condividere il framework.

Risorse aggiuntive

- Nella pagina dei dettagli del mio framework personalizzato, mi viene richiesto di ricreare il mio framework personalizzato
- Non riesco a creare una copia del mio framework personalizzato o utilizzarlo per creare una valutazione

Creazione di un framework personalizzato in AWS Audit Manager

Puoi utilizzare framework personalizzati per organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici.

Punti chiave

Quando si tratta di creare framework personalizzati in Audit Manager, è possibile scegliere tra due metodi:

1. Creazione di un framework personalizzato partendo da zero: in questo modo avrete la flessibilità di iniziare da zero e definire ogni aspetto del framework in base alle vostre specifiche. Questo approccio è particolarmente utile quando i requisiti si discostano in modo significativo dai framework standard esistenti o quando è necessario incorporare set di controllo proprietari specifici per l'organizzazione.
2. Creazione di una copia modificabile di un framework esistente: questo approccio consente di sfruttare la struttura e il contenuto di un framework esistente, offrendo al contempo la libertà di personalizzarlo in base alle proprie esigenze specifiche. Partendo da una base consolidata, è possibile semplificare il processo di creazione del framework personalizzato, concentrando gli sforzi sulla sua personalizzazione in base ai requisiti specifici dell'organizzazione.

Indipendentemente dall'approccio scelto, la creazione di un framework personalizzato prevede una serie di passaggi come la specificazione dei dettagli del framework, la definizione dei set di controlli e la revisione del framework prima di finalizzarne la creazione. Durante questo processo, è possibile incorporare i set di controllo specifici dell'organizzazione, assicurando che il framework personalizzato rifletta accuratamente i requisiti GRC.

Risorse aggiuntive

Per istruzioni su come creare un framework personalizzato, consulta le seguenti risorse.

- Creare un framework personalizzato partendo da zero in AWS Audit Manager
- Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Creare un framework personalizzato partendo da zero in AWS Audit Manager

Quando i requisiti di conformità dell'organizzazione non sono in linea con i framework standard predefiniti disponibili in AWS Audit Manager, è possibile creare un framework personalizzato partendo da zero.

Questa pagina descrive i passaggi per creare un framework personalizzato su misura per le tue esigenze specifiche.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per creare un framework personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Attività

- Fase 1: specificare i dettagli del framework
- Fase 2: Specificare i set di controllo
- Fase 3: Revisione e creazione del framework

Fase 1: specificare i dettagli del framework

Inizia specificando i dettagli sul tuo framework personalizzato.

Per specificare i dettagli del framework

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Libreria Framework, quindi scegli Crea framework personalizzato.
3. In Dettagli del framework, inserisci un nome, un tipo di conformità (opzionale) e una descrizione per il tuo framework (anch'essa facoltativa). L'immissione di un tipo di conformità come PCI_DSS o GDPR significa che puoi utilizzare questa parola chiave per cercare il tuo framework in un secondo momento.
4. Nella sezione Tag, scegli Aggiungi nuovo tag per associare un tag al tuo framework. Per ogni tag è possibile specificare una chiave e un valore. La chiave del tag è obbligatoria. Puoi utilizzarla come criterio di ricerca quando cerchi questo framework nella libreria del framework.

5. Seleziona Successivo.

Fase 2: Specificare i set di controllo

Successivamente, specifichi quali controlli desideri aggiungere al tuo framework e come desideri organizzarli. Inizia aggiungendo set di controlli al framework, quindi aggiungi controlli al set di controlli.

> **Note**
>
> Quando si utilizza la AWS Audit Manager console per creare un framework personalizzato, è possibile aggiungere fino a 10 set di controlli per ogni framework.
> Quando utilizzi l'API Gestione audit per creare un framework personalizzato, puoi creare più di 10 set di controlli. Per aggiungere più set di controlli rispetto a quelli attualmente consentiti dalla console, utilizza l'CreateAssessmentFrameworkAPI fornita da Audit Manager.

Per specificare un set di controlli

1. Nella sezione Nome del set di controllo, inserisci un nome per il set di controlli.
2. In Aggiungi controlli, utilizza l'elenco a discesa Tipo di controllo per selezionare uno dei due tipi di controllo: controlli standard o controlli personalizzati.
3. In base all'opzione selezionata nel passaggio precedente, viene visualizzato un elenco di controlli standard o controlli personalizzati. Seleziona uno o più controlli e scegli Aggiungi al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi al set di controlli.
5. Controlla i controlli che appaiono nell'elenco dei controlli selezionati.
   - Per aggiungere altri controlli, ripetere i passaggi da 2 a 4.
   - Per rimuovere i controlli indesiderati, seleziona uno o più controlli e scegli Rimuovi controllo.
6. Per aggiungere un nuovo set di controlli, scegli Aggiungi set di controlli.
7. Per rimuovere un set di controlli indesiderato, scegli Rimuovi set di controlli.
8. Dopo aver aggiunto i set di controlli e i controlli, seleziona Successivo.

Fase 3: Revisione e creazione del framework

Rivedi le informazioni del tuo framework. Per modificare le informazioni relative a una fase, scegli Modifica.

Al termine, scegli Crea framework personalizzato.

Passaggi successivi

Dopo aver creato il nuovo framework personalizzato, puoi creare una valutazione a partire dal tuo framework. Per ulteriori informazioni, consulta Creazione di una valutazione in AWS Audit Manager.

Per rivisitare il framework personalizzato in un secondo momento, consultaIndividuazione dei framework disponibili in AWS Audit Manager. Puoi seguire questi passaggi per individuare il framework personalizzato in modo da poterlo quindi visualizzare, modificare, condividere o eliminare.

Risorse aggiuntive

Per le soluzioni ai problemi del framework in Audit Manager, vedereRisoluzione dei problemi relativi al framework.

Creazione di una copia modificabile di un framework esistente in AWS Audit Manager

Invece di creare un framework personalizzato da zero, è possibile utilizzare un framework esistente come punto di partenza e crearne una copia modificabile. Quando si esegue questa operazione, il framework esistente rimane nella libreria del framework e viene creato un nuovo framework personalizzato con le impostazioni specifiche dell'utente.

È possibile creare una copia modificabile di qualsiasi framework esistente. Può essere un framework standard o un framework personalizzato.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per creare un framework personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Attività

- Fase 1: specificare i dettagli del framework
- Fase 2: Specificare i set di controllo
- Fase 3: Revisione e creazione del framework

Fase 1: specificare i dettagli del framework

Tutti i dettagli del framework, tranne i tag, vengono trasferiti dal framework originale. Esamina e modifica questi dettagli in base alle esigenze.

Per specificare i dettagli del framework

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Libreria Framework.
3. Scegliete il framework che desiderate utilizzare come punto di partenza, scegliete Crea un framework personalizzato, quindi scegliete Crea una copia.
4. Nella finestra pop-up che appare, inserisci un nome per il nuovo framework personalizzato e scegli Continua.
5. In Dettagli del framework, esamina il nome, il tipo di conformità e la descrizione del framework e modificali se necessario. Il tipo di conformità deve indicare lo standard di conformità o il regolamento associato al framework. Puoi usare questa parola chiave per cercare il tuo framework.
6. Nella sezione Tag, scegli Aggiungi nuovo tag per associare un tag al tuo framework. Per ogni tag è possibile specificare una chiave e un valore. La chiave tag è obbligatoria e può essere utilizzata come criterio di ricerca quando si cerca questo framework nella libreria del framework.
7. Seleziona Successivo.

Fase 2: Specificare i set di controllo

I set di controllo vengono trasferiti dal framework originale. Modifica la configurazione corrente aggiungendo altri controlli o rimuovendo i controlli esistenti in base alle esigenze.

> **Note**
>
> Quando si utilizza la console Audit Manager per creare un framework personalizzato, è possibile aggiungere fino a 10 set di controlli per ogni framework.
> Quando utilizzi l'API Gestione audit per creare un framework personalizzato, puoi aggiungere più di 10 set di controlli. Per aggiungere più set di controlli rispetto a quelli attualmente consentiti dalla console, utilizza l'CreateAssessmentFrameworkAPI fornita da Audit Manager.

Per specificare un set di controlli

1. In Nome del set di controllo, modificate il nome del set di controlli in base alle esigenze.
2. In Aggiungi controlli, aggiungi un nuovo controllo utilizzando l'elenco a discesa per selezionare uno dei due tipi di controllo: controlli standard o controlli personalizzati.
3. In base all'opzione selezionata nel passaggio precedente, viene visualizzato un elenco di controlli standard o controlli personalizzati. Seleziona uno o più controlli e scegli Aggiungi al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi al set di controlli.
5. Controlla i controlli che appaiono nell'elenco dei controlli selezionati.
   - Per aggiungere altri controlli, ripetere i passaggi da 2 a 4.
   - Per rimuovere i controlli indesiderati, seleziona uno o più controlli e scegli Rimuovi controllo.
6. Per aggiungere un nuovo set di controlli al framework, scegli Aggiungi set di controlli.
7. Per rimuovere un set di controlli indesiderato, scegliete Rimuovi set di controllo.
8. Dopo aver aggiunto i set di controlli e i controlli, seleziona Successivo.

Fase 3: Revisione e creazione del framework

Rivedi le informazioni del tuo framework. Per modificare le informazioni relative a una fase, scegli Modifica.

Al termine, scegli Crea framework personalizzato.

Passaggi successivi

Dopo aver creato il nuovo framework personalizzato, puoi creare una valutazione a partire dal tuo framework. Per ulteriori informazioni, consulta Creazione di una valutazione in AWS Audit Manager.

Per rivisitare il framework personalizzato in un secondo momento, consultaIndividuazione dei framework disponibili in AWS Audit Manager. Puoi seguire questi passaggi per individuare il framework personalizzato in modo da poterlo quindi visualizzare, modificare, condividere o eliminare.

Risorse aggiuntive

Per le soluzioni ai problemi del framework in Audit Manager, vedereRisoluzione dei problemi relativi al framework.

Modifica di un framework personalizzato in AWS Audit Manager

Potrebbe essere necessario modificare i framework personalizzati man mano che cambiano AWS Audit Manager i requisiti di conformità.

Questa pagina descrive i passaggi per modificare i dettagli e i set di controlli di un framework personalizzato.

Prerequisiti

La procedura seguente presuppone che sia stato precedentemente creato un framework personalizzato.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per modificare un framework personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Attività

- Fase 1: modificare dettagli del framework
- Fase 2: Modifica dei set di controllo
- Fase 3. Rivedi e salva

Fase 1: modificare dettagli del framework

Inizia esaminando e modificando i dettagli del framework esistente.

Per modificare i dettagli del framework

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione a sinistra, scegli Libreria Framework e scegli la scheda Framework personalizzati.
3. Seleziona il framework che si desideri modificare, scegli Azioni, quindi scegli Modifica.
   - In alternativa, apri un framework personalizzato e scegli Modifica in alto a destra nella pagina dei dettagli del framework.
4. In Dettagli del framework, esamina il nome, il tipo di conformità e la descrizione del framework e apporta le modifiche necessarie.
5. Seleziona Successivo.

> **Tip**
>
> Per modificare i tag per un framework, apri il framework e scegli la scheda dei tag del framework. Qui puoi visualizzare e modificare i tag associati al framework.

Fase 2: Modifica dei set di controllo

Successivamente, rivedi e modifica i controlli e i set di controlli nel framework.

> **Note**
>
> Quando si utilizza la AWS Audit Manager console per modificare un framework personalizzato, è possibile aggiungere fino a 10 set di controlli per ogni framework. Quando utilizzi l'API Gestione audit per modificare un framework personalizzato, puoi aggiungere più di 10 set di controlli. Per aggiungere più set di controlli rispetto a quelli attualmente consentiti dalla console, utilizza l'UpdateAssessmentFrameworkAPI fornita da Audit Manager.

Per modificare un set di controlli

1. Nella sezione Nome del set di controlli, rivedi e modifica il nome del set di controlli secondo le necessità.

2. In Aggiungi controlli, utilizza l'elenco a discesa Tipo di controllo per selezionare uno dei due tipi di controllo: controlli standard o controlli personalizzati.
3. In base all'opzione selezionata nel passaggio precedente, viene visualizzato un elenco a tabella di controlli standard o controlli personalizzati. Seleziona uno o più controlli e scegli Aggiungi al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi.
5. Rivedi e modifica i controlli visualizzati nell'elenco dei controlli selezionati.
   - Per aggiungere altri controlli, ripetere i passaggi da 2 a 4.
   - Per rimuovere i controlli indesiderati, seleziona uno o più controlli e scegli Rimuovi dal set di controlli.
6. Per aggiungere un nuovo set di controlli al framework, scegli Aggiungi set di controlli.
7. Per rimuovere un set di controlli indesiderato, scegliete Rimuovi set di controllo.
8. Dopo aver aggiunto i set di controlli e i controlli, seleziona Successivo.

Fase 3. Rivedi e salva

Rivedi le informazioni del tuo framework. Per modificare le informazioni relative a una fase, scegli Modifica.

Al termine, scegli Salva le modifiche.

Passaggi successivi

Quando sei sicuro di non aver più bisogno di un framework personalizzato, puoi ripulire il tuo ambiente Audit Manager eliminando il framework. Per istruzioni, consulta Eliminazione di un framework personalizzato in AWS Audit Manager.

Risorse aggiuntive

Per le soluzioni ai problemi del framework in Audit Manager, vedereRisoluzione dei problemi relativi al framework.

Condivisione di un framework personalizzato in AWS Audit Manager

Puoi utilizzare la funzionalità di condivisione del framework per AWS Audit Manager replicare rapidamente i framework personalizzati che crei. Puoi condividere i tuoi framework personalizzati con altri o replicare i tuoi framework in un altro Account AWS con il tuo account. Regione AWS Il destinatario può quindi accedere al framework personalizzato e utilizzarlo per creare valutazioni. Può farlo senza dover ripetere le operazioni di configurazione per quel framework.

Punti chiave

Per condividere un framework personalizzato, è necessario creare una richiesta di condivisione. Il destinatario della richiesta di condivisione ha 120 giorni di tempo per accettare o rifiutare la richiesta. Se il destinatario accetta la richiesta di condivisione, Gestione audit replica il framework personalizzato condiviso nella sua libreria di framework. Oltre a replicare il framework personalizzato, Gestione audit replica anche tutti i set di controlli e i controlli personalizzati contenuti in tale framework. I controlli personalizzati vengono dunque aggiunti alla libreria di controlli del destinatario. Gestione audit non replica framework o controlli standard. Per impostazione predefinita, sono disponibili in tutti gli Account AWS e le regioni in cui è abilitato Gestione audit.

La funzionalità di condivisione del framework è disponibile solo nel piano a pagamento. Tuttavia, non sono previsti costi aggiuntivi per la condivisione di un framework personalizzato o l'accettazione di una richiesta di condivisione. Per ulteriori informazioni sui prezzi di AWS Audit Manager, consulta la pagina dei prezzi.AWS Audit Manager

> **Important**
>
> Non puoi condividere un framework personalizzato derivato da un framework standard se il framework standard è indicato come non idoneo alla condivisione da AWS, a meno che tu non abbia ottenuto l'autorizzazione in tal senso dal proprietario del framework standard. Per vedere quali framework standard non sono idonei alla condivisione e per ulteriori informazioni, consulta Idoneità alla condivisione del framework.

Risorse aggiuntive

Per ulteriori informazioni su come condividere framework personalizzati in Audit Manager, consulta le seguenti risorse.

- Concetti e terminologia di condivisione dei framework
- Invio di una richiesta di condivisione di un framework personalizzato in AWS Audit Manager

- Rispondere alle richieste di condivisione in AWS Audit Manager
- Eliminazione delle richieste di condivisione in AWS Audit Manager

Concetti e terminologia di condivisione dei framework

Se impari a conoscere i seguenti concetti chiave, puoi ottenere di più dalla funzionalità di condivisione del framework personalizzato AWS Audit Manager .

Punti chiave

Mittente

Questo è il creatore di una richiesta di condivisione e il Account AWS luogo in cui esiste il framework personalizzato. I mittenti possono condividere framework personalizzati con chiunque. Account AWS Oppure, replicano un framework personalizzato su qualsiasi framework supportato dal proprio Regione AWS account.

Destinatario

Si tratta del consumatore del framework condiviso. I destinatari possono accettare o rifiutare una richiesta di condivisione da parte di un mittente.

> **Note**
>
> Un destinatario può essere un account da amministratore delegato. Tuttavia, non è possibile condividere framework personalizzati con un AWS Organizations account di gestione.

Idoneità al framework

È possibile condividere solo framework personalizzati. Per impostazione predefinita, i framework standard sono già presenti in tutti Account AWS e Regioni AWS dove sono abilitati. AWS Audit Manager Inoltre, i framework personalizzati che condividi non devono contenere dati sensibili. Tra essi figurano i dati trovati all'interno del framework stesso, i relativi set di controlli e tutti i controlli personalizzati che fanno parte del framework personalizzato.

> **Important**
>
> Alcuni dei framework standard offerti da AWS Audit Manager contengono materiale protetto da copyright soggetto a contratti di licenza. I framework personalizzati possono contenere contenuti derivati da questi framework. Non puoi condividere un framework personalizzato derivato da un framework standard se il framework standard è indicato come non idoneo alla condivisione da AWS, a meno che tu non abbia ottenuto l'autorizzazione in tal senso dal proprietario del framework standard.
> Per sapere quali framework standard sono idonei alla condivisione, consulta la tabella seguente.

Nome del framework standard	Versioni personalizzate idonee alla condivisione
Essential Eight dell'Australian Cyber Security Center (ACSC)	 Sì
Manuale sulla sicurezza delle informazioni (ISM) dell'Australian Cyber Security Center (ACSC) 02 marzo 2023	 Sì
Framework di esempio di Amazon Web Services (AWS) Audit Manager	 Sì
AWS Control Tower Guardrail	 Sì
AWS framework generativo di best practice per l'intelligenza artificiale v2	 Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione
AWS License Manager	 Sì
AWS Best practice di sicurezza di base	 Sì
AWS Migliori pratiche operative	 Sì
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	 Sì
Medium Cloud Control del Centro canadese per la sicurezza informatica (CCCS)	 No
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, livello 1	 No
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, livello 1 e 2	 No
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, livello 1	 No

Nome del framework standard	Versioni personalizzate idonee alla condivisione
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, livello 1 e 2	 No
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, livello 1	 No
Centro per la sicurezza Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, livello 1 e 2	 No
Centro per la sicurezza Internet (CIS) v7.1, IG1	 Sì
CIS Critical Security Controls versione 8.0 (CIS v8.0), IG1	 No
Controlli di base sulla sicurezza del Federal Risk and Authorization Management Program (FedRAMP) r4, Moderate	 Sì
Regolamento generale sulla protezione dei dati (GDPR) 2016	 Sì
Gramm-Leach-Bliley Act (GLBA)	 Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione	
Titolo 21 Codice dei regolamenti federali (CFR), parte 11, Registri elettronici; firme elettroniche: ambito di applicazione e applicazione 24 maggio 2023		Sì
EudraLex - Le norme che disciplinano i medicinali nell'Unione europea (UE) - Volume 4: Medicinali di buona fabbricazione (GMP) per uso umano e veterinario - Allegato 11		Sì
Norma di sicurezza dell'Health Insurance Portability and Accountability Act (HIPAA): febbraio 2003		Sì
Regola finale omnibus dell'Health Insurance Portability and Accountability Act (HIPAA)		Sì
Organizzazione internazionale per la standardizzazione (ISO) /Commissione elettrotecnica internazionale (IEC) 27001:2013 Allegato A		No
NIST 800-53 Rev 5: Controlli di sicurezza e privacy per sistemi informativi e organizzazioni		Sì
NIST Cybersecurity Framework (CSF) v1.1		Sì
NIST 800-171 Revisione 2: Protezione delle informazioni non classificate controllate in sistemi e organizzazioni non federali		Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	 No
Standard di sicurezza dei dati del settore delle carte di pagamento (PCI DSS) v4.0	 No
Dichiarazione sugli Standard for Attestations Engagement (SSAE) n. 18, Service Organizations Controls (SOC) Report 2	 No

Richiesta di condivisione

Per condividere un framework personalizzato, è necessario creare una richiesta di condivisione. La richiesta di condivisione specifica un destinatario e lo avvisa della disponibilità di un framework personalizzato. I destinatari hanno 120 giorni di tempo per rispondere a una richiesta di condivisione accettandola o rifiutandola. Se non viene intrapresa alcuna azione entro 120 giorni, la richiesta di condivisione scade e il destinatario perde la possibilità di aggiungere il framework personalizzato alla propria libreria di framework. I mittenti e i destinatari possono visualizzare e agire sulle richieste di condivisione dalla pagina delle richieste di condivisione della libreria di framework.

Stato della richiesta di condivisione

Le richieste di condivisione possono avere uno dei seguenti stati.

Stato	Descrizione
Active (Attivo)	Indica una richiesta di condivisione che è stata inviata correttamente al destinatario ed è in attesa della sua risposta.
In scadenza	Ciò indica una richiesta di condivisione che scade entro i prossimi 30 giorni.

Stato	Descrizione
Condiviso	Indica una richiesta di condivisione accettata dal destinatario.
Inattivo	Indica una richiesta di condivisione che è stata revocata, rifiutata o scaduta prima che il destinatario agisse.
Replica	Ciò indica una richiesta di condivisione accettata che viene replicata nella libreria di framework del destinatario.
Failed (Non riuscito)	Ciò indica una richiesta di condivisione che non è stata inviata correttamente al destinatario.

Notifiche di richiesta di condivisione

Gestione audit avvisa i destinatari quando ricevono una richiesta di condivisione. Sia i destinatari che i mittenti ricevono una notifica quando una richiesta di condivisione sta per scadere nei prossimi 30 giorni.

- Per i destinatari, accanto alle richieste ricevute con stato Attive o In scadenza. Il destinatario può risolvere la notifica accettando o rifiutando la richiesta di condivisione.
- Per i mittenti, accanto alle richieste ricevute con stato In scadenza appare un punto di notifica di colore blu. Il destinatario può risolvere la notifica accettando o rifiutando la richiesta. Altrimenti, viene risolta alla scadenza della richiesta. Inoltre, il mittente può risolvere la notifica revocando la richiesta di condivisione.

Titolarità del mittente

I mittenti mantengono l'accesso completo ai framework personalizzati che condividono. Possono annullare le richieste di condivisione attive in qualsiasi momento revocando la richiesta di condivisione prima della scadenza. Tuttavia, una volta che un destinatario ha accettato una richiesta di condivisione, il mittente non può più revocare l'accesso del destinatario a quel framework personalizzato. Questo perché quando il destinatario accetta la richiesta, Gestione audit crea una copia indipendente del framework personalizzato nella libreria del framework del destinatario.

Oltre a replicare il framework personalizzato del mittente, Gestione audit replica anche tutti i set di controlli e i controlli personalizzati contenuti in tale framework. Tuttavia, Gestione audit non replica alcun tag collegato al framework personalizzato.

Titolarità del destinatario

I destinatari hanno pieno accesso ai framework personalizzati che accettano. Quando il destinatario accetta la richiesta, Gestione audit replica il framework personalizzato nella scheda framework personalizzati della propria libreria di framework. I destinatari possono quindi gestire il framework personalizzato condiviso nello stesso modo in cui si usa qualsiasi altro framework personalizzato. I destinatari possono condividere i framework personalizzati che ricevono da altri mittenti. I destinatari non possono impedire ai mittenti di inviare richieste di condivisione.

Scadenza del framework condiviso

Quando un mittente crea una richiesta di condivisione, Gestione audit imposta la scadenza della richiesta dopo 120 giorni. I destinatari possono accettare e accedere al framework condiviso prima della scadenza della richiesta. Se un destinatario non accetta durante questo periodo, la richiesta di condivisione scade. Dopo questo momento, una registrazione della richiesta di condivisione scaduta rimane nella loro cronologia. Le istantanee dei framework condivisi scaduti vengono archiviate in un bucket S3 con un TTL di un anno a scopo di controllo.

I mittenti possono scegliere di revocare una richiesta di condivisione in qualsiasi momento prima della scadenza.

Archiviazione e backup dei dati del framework condiviso

Quando si crea una richiesta di condivisione, Audit Manager archivia un'istantanea del framework personalizzato negli Stati Uniti orientali (Virginia settentrionale). Regione AWS Audit Manager archivia anche un backup della stessa istantanea negli Stati Uniti occidentali (Oregon). Regione AWS

Gestione audit elimina lo snapshot e lo snapshot di backup quando si verifica uno dei seguenti eventi:

- Il mittente revoca la richiesta di condivisione.
- Il destinatario rifiuta la richiesta di condivisione.
- Il destinatario riscontra un errore e non accetta correttamente la richiesta di condivisione.
- La richiesta di condivisione scade prima che il destinatario risponda alla richiesta.

Quando un mittente invia nuovamente una richiesta di condivisione, l'istantanea viene sostituita con una versione aggiornata che corrisponde alla versione più recente del framework personalizzato.

Quando un destinatario accetta una richiesta di condivisione, l'istantanea viene replicata nel destinatario in Account AWS base a quanto specificato nella richiesta di condivisione. Regione AWS

Controllo delle versioni del framework condiviso

Quando si condivide un framework personalizzato, Audit Manager crea una copia indipendente di tale framework nella regione Account AWS e specificata. Ciò significa che è necessario considerare quanto segue:

- Il framework condiviso accettato da un destinatario è un'istantanea del framework al momento della creazione della richiesta di condivisione. Se aggiorni il framework personalizzato originale dopo aver inviato una richiesta di condivisione, la richiesta non viene aggiornata automaticamente. Per condividere l'ultima versione del framework aggiornato, puoi inviare nuovamente la richiesta di condivisione. La data di scadenza di questa nuova istantanea è di 120 giorni dalla data di ricondivisione.
- Quando condividi un framework personalizzato con un altro Account AWS e poi lo elimini dalla tua libreria di framework, il framework personalizzato condiviso rimane nella libreria framework del destinatario.
- Quando condividi un framework personalizzato Regione AWS con un altro tramite il tuo account e poi elimini quel framework personalizzato nel primo Regione AWS, il framework personalizzato rimane nella seconda regione.
- Quando elimini un framework personalizzato condiviso dopo averlo accettato, tutti i controlli personalizzati che sono stati replicati come parte del framework personalizzato rimangono nella tua libreria di controlli.

Risorse aggiuntive

- Invio di una richiesta di condivisione di un framework personalizzato in AWS Audit Manager
- Rispondere alle richieste di condivisione in AWS Audit Manager
- Eliminazione delle richieste di condivisione in AWS Audit Manager
- Risoluzione dei problemi relativi al framework

Invio di una richiesta di condivisione di un framework personalizzato in AWS Audit Manager

Questo tutorial descrive come condividere i framework personalizzati tra Account AWS e. Regioni AWS

Quando condividi un framework personalizzato, Gestione audit crea un'istantanea del framework e invia una richiesta di condivisione al destinatario. Il destinatario ha 120 giorni per accettare il framework condiviso. Se il destinatario accetta, Gestione audit replica il framework personalizzato condiviso nella sua libreria di framework nella Regione AWS specificata. Se desideri replicare un framework personalizzato in un'altra regione con il tuo account, usa il seguente tutorial e inserisci il tuo Account AWS ID come ID dell'account del destinatario.

Prerequisiti

Prima di iniziare questo tutorial, assicurati che siano soddisfatte le seguenti condizioni:

- Conosci il framework che condivide concetti e terminologia Gestione audit.
- Il framework personalizzato che desideri condividere è idoneo alla condivisione ed è presente nella libreria di framework del tuo ambiente AWS Audit Manager .
- Il destinatario è già abilitato AWS Audit Manager nel Regione AWS luogo in cui desideri condividere il framework personalizzato.
- Il destinatario non è un account AWS Organizations di gestione.
- La tua identità IAM dispone delle autorizzazioni appropriate per condividere un framework personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

> **Tip**
>
> Prima di iniziare, prendi nota dell' Account AWS ID con cui desideri condividere il framework personalizzato. Questo può essere l'ID del tuo account, se il tuo obiettivo è replicare il framework su un altro del tuo Regione AWS account. Queste informazioni serviranno per la fase 2 del tutorial.

Procedura

Attività

- Fase 1: Identificare il framework personalizzato da condividere
- Fase 2: inviare una richiesta di condivisione
- Fase 3: visualizzazione delle richieste inviate
- Fase 4 (facoltativo): revoca della richiesta di condivisione

Fase 1: Identificare il framework personalizzato da condividere

Inizia identificando il framework personalizzato da condividere. Puoi visualizzare un elenco di tutti i framework disponibili nella pagina della libreria Framework in Gestione audit.

> **Important**
>
> Non condividere framework personalizzati che contengono dati sensibili. Tra essi figurano i dati trovati all'interno del framework stesso, i relativi set di controlli e tutti i controlli personalizzati che fanno parte del framework personalizzato. Per ulteriori informazioni, consulta Idoneità al framework.

Per visualizzare i framework personalizzati disponibili

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Libreria Framework.
3. Scegli la scheda Framework personalizzati. Viene visualizzato un elenco dei framework personalizzati disponibili. Puoi scegliere un nome di framework per visualizzarne i dettagli.

Fase 2: inviare una richiesta di condivisione

Successivamente, specifica un destinatario e inviagli una richiesta di condivisione per il framework personalizzato. Il destinatario ha 120 giorni per rispondere alla richiesta di condivisione prima che scada.

Per inviare una richiesta di condivisione

1. Dalla scheda Framework personalizzati della libreria di framework, scegli il nome di un framework per aprire la pagina dei dettagli. Da qui, scegli Azioni, quindi scegli Condividi framework personalizzato.
   - In alternativa, seleziona un framework personalizzato dall'elenco nella libreria del framework, scegli Azioni, quindi scegli Condividi framework personalizzato. A seconda delle dimensioni del framework personalizzato, questo metodo può richiedere alcuni secondi mentre Gestione audit prepara la richiesta di condivisione.
2. Rivedere l'avviso visualizzato nella finestra di dialogo.
   - Se non sei sicuro di poter condividere il tuo framework personalizzato, consulta idoneità al Framework per ulteriori indicazioni.
   - Se il tuo framework dispone di controlli che utilizzano AWS Config regole personalizzate come fonte di dati, ti consigliamo di contattare il destinatario per informarlo. Il destinatario può quindi creare e abilitare le stesse AWS Config regole nella propria istanza di AWS Config. Per ulteriori informazioni, consulta Il mio framework condiviso dispone di controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?.
3. Inserisci **`agree`** e scegli Accetta per procedere.
4. Nella schermata successiva, esegui le operazioni seguenti:
   - Nella sezione Account AWS, inserisci l'ID dell'account del destinatario. Può essere il tuo ID account.
   - Nella sezione Regione AWS, seleziona la regione del destinatario dall'elenco a discesa.
   - (Facoltativo) Nella sezione Messaggio al destinatario, inserisci un commento facoltativo sul framework personalizzato che stai condividendo.
   - Nella sezione Dettagli del framework personalizzato, rivedi i dettagli per confermare che desideri condividere questo framework.
5. Scegli Condividi.

> **Note**
>
> Tieni presenti le informazioni seguenti:

- Quando condividi un framework personalizzato con un altro Account AWS, il framework viene replicato solo nella versione specificata Regione AWS. Dopo aver accettato la richiesta di condivisione, il destinatario può quindi replicare il framework tra le regioni, se necessario.
- Quando si condividono framework personalizzati Regioni AWS, possono essere necessari fino a 10 minuti per elaborare le azioni di richiesta di condivisione. Dopo aver inviato una richiesta di condivisione tra aree geografiche, ti consigliamo di ricontrollare in un secondo momento per confermare che la richiesta di condivisione è stata inviata correttamente.
- Quando invii una richiesta di condivisione, Gestione audit scatta un'istantanea del framework personalizzato al momento della creazione della richiesta di condivisione. Se aggiorni il framework personalizzato dopo aver inviato una richiesta di condivisione, la richiesta non viene aggiornata automaticamente. Per condividere l'ultima versione di un framework aggiornato, puoi inviare nuovamente la richiesta di condivisione. La data di scadenza di questa nuova istantanea è di 120 giorni dalla data di ricondivisione.

Fase 3: visualizzazione delle richieste inviate

Puoi selezionare la scheda Richieste inviate per visualizzare un elenco di tutte le richieste di condivisione che hai inviato. Puoi filtrare questo elenco in base alle tue esigenze. Ad esempio, puoi applicare filtri per visualizzare solo le richieste che scadono entro i prossimi 30 giorni.

Per visualizzare e filtrare le richieste inviate

1. Nel riquadro di navigazione, scegli Richieste di condivisione.
2. Scegli la scheda Richieste inviate.
3. (Facoltativo) Applica filtri per definire quali richieste inviate sono visibili. Puoi farlo cercando l'elenco a discesa Tutti gli stati e modificando il filtro impostandolo su uno dei seguenti.

Stato	Descrizione
Active (Attivo)	Questo filtro mostra le richieste di condivisione in attesa di risposta dal destinatario.
In scadenza	Questo filtro mostra le richieste di condivisione che scadono nei prossimi 30 giorni.

Stato	Descrizione
Condiviso	Questo filtro mostra le richieste di condivisione accettate dal destinatario. Il framework personalizzato condiviso ora esiste nella libreria di framework del destinatario.
Inattivo	Questo filtro mostra le richieste di condivisione che sono state rifiutate, revocate o scadute prima che il destinatario agisse. Scegli la parola Inattivo per visualizzare ulteriori dettagli.
Replica	Ciò indica una richiesta di condivisione accettata che viene replicata nella libreria di framework del destinatario.
Failed (Non riuscito)	Questo filtro mostra le richieste di condivisione che non sono state inviate correttamente al destinatario. Scegli la parola Non riuscito per visualizzare ulteriori dettagli.

> **Note**
>
> L'elaborazione di una richiesta di condivisione può richiedere fino a 15 minuti. Di conseguenza, se si verifica un errore durante l'invio della richiesta di condivisione al destinatario, lo stato Non riuscito potrebbe non essere visualizzato immediatamente. T consigliamo di ricontrollare in un secondo momento per confermare che la richiesta di condivisione è stata inviata correttamente.

Fase 4 (facoltativo): revoca della richiesta di condivisione

Se devi annullare una richiesta di condivisione attiva prima della scadenza, puoi revocarla in qualsiasi momento. Questa fase è facoltativa. Se non intraprendi alcuna azione, il destinatario perde la possibilità di accettare la richiesta di condivisione dopo la data di scadenza.

Per revocare una richiesta di condivisione

1. Nel riquadro di navigazione, scegli Richieste di condivisione.
2. Scegli la scheda Richieste inviate.
3. Seleziona il framework che desideri revocare e scegli Revoca richiesta.

4. Nella finestra pop-up che appare, scegli Revoca.

> **Note**
>
> Puoi revocare l'accesso solo alle richieste di condivisione con lo stato Attive o In scadenza. Una volta che un destinatario ha accettato una richiesta di condivisione, non puoi più revocargli l'accesso a quel framework personalizzato. Questo perché una copia del framework personalizzato ora esiste nella libreria del framework del destinatario.
> Quando si condividono framework tra più framework Regioni AWS, l'elaborazione delle azioni di richiesta di condivisione può richiedere fino a 10 minuti. Dopo aver revocato una richiesta di condivisione tra aree geografiche, ti consigliamo di ricontrollare in un secondo momento per confermare che la richiesta di condivisione è stata revocata correttamente.

Passaggi successivi

Reinvio di una richiesta di condivisione per un framework aggiornato

Puoi inviare una richiesta di condivisione per un framework personalizzato e poi aggiornare lo stesso framework in seguito. In tal caso, la richiesta di condivisione non viene aggiornata automaticamente e non riflette l'ultima versione del framework. Tuttavia, se il suo stato è attive, condivise o in scadenza, puoi aggiornare una richiesta di condivisione esistente. A tale scopo, invii nuovamente una nuova richiesta di condivisione con lo stesso set di dettagli della richiesta esistente. Nella nuova richiesta di condivisione, includi lo stesso ID del framework personalizzato, l'ID dell'account del destinatario e la stessa Regione AWS destinatario. Puoi anche fornire un nuovo commento con la nuova richiesta di condivisione.

Quando invii nuovamente una richiesta di condivisione, tieni presente quanto segue:

- Affinché l'aggiornamento abbia esito positivo, la nuova richiesta deve riguardare lo stesso ID del framework personalizzato. Deve inoltre specificare lo stesso ID account del destinatario e la stessa regione della richiesta esistente.
- Se il nome del framework personalizzato è cambiato, nella richiesta di condivisione aggiornata viene visualizzato il nome più recente.
- Se fornisci un nuovo commento, nella richiesta di condivisione aggiornata viene visualizzato il commento più recente.

- Quando invii nuovamente una richiesta di condivisione, la data di scadenza viene prorogata di sei mesi.

Per inviare nuovamente una richiesta di condivisione per un framework aggiornato

1. Dalla scheda Framework personalizzati della libreria di framework, scegli il nome di un framework che vuoi condividere. Si apre la pagina dei dettagli del framework.
2. Scegli Azioni, quindi scegli Condividi framework personalizzato.
3. Esamina l'avviso visualizzato nella finestra di dialogo, inserisci **`agree`**, quindi scegli Accetto per procedere.
4. Nella schermata successiva, esegui le operazioni seguenti:
   - Nella sezione Account AWS, inserisci lo stesso ID account che hai specificato nella richiesta di condivisione esistente.
   - Nella sezione Regione AWS, seleziona la stessa regione che hai specificato nella richiesta di condivisione esistente.
   - (Facoltativo) Nella sezione Messaggio al destinatario, inserisci un commento facoltativo sul framework personalizzato aggiornato.
   - Nella sezione Dettagli del framework personalizzato, rivedi i dettagli per confermare che desideri inviare nuovamente la richiesta di condivisione.
5. Scegli Condividi per inviare nuovamente e aggiornare la richiesta di condivisione.

Risorse aggiuntive

Per trovare soluzioni ai problemi che potresti riscontrare quando condividi un framework personalizzato, consultaRisoluzione dei problemi relativi al framework.

Rispondere alle richieste di condivisione in AWS Audit Manager

Questo tutorial descrive le azioni da eseguire quando ricevi una richiesta di condivisione per un framework personalizzato. Gestione audit ti avvisa quando ricevi una richiesta di condivisione. Riceverai una notifica anche quando una richiesta di condivisione sta per scadere nei prossimi 30 giorni.

Prerequisiti

Prima di iniziare, ti consigliamo di approfondire la condivisione dei concetti e della terminologia del framework Gestione audit.

Procedura

Attività

- Fase 1: verifica delle notifiche di richiesta ricevute
- Fase 2: Intervenire sulla richiesta
- Fase 3: visualizzazione di una cronologia delle richieste ricevute

Fase 1: verifica delle notifiche di richiesta ricevute

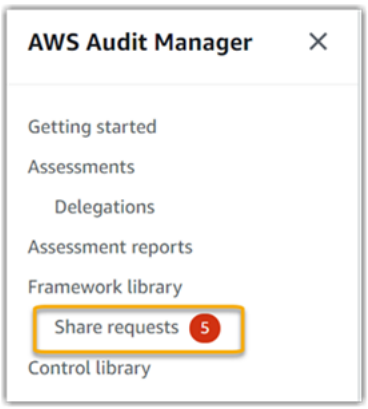
Inizia controllando le notifiche di richiesta di condivisione. La scheda Richieste ricevute mostra un elenco delle richieste di condivisione che hai ricevuto da altri Account AWS. Le richieste in attesa di risposta vengono visualizzate con un punto blu. Puoi anche filtrare questa visualizzazione per visualizzare solo le richieste che scadono entro i prossimi 30 giorni.

Per visualizzare le richieste ricevute

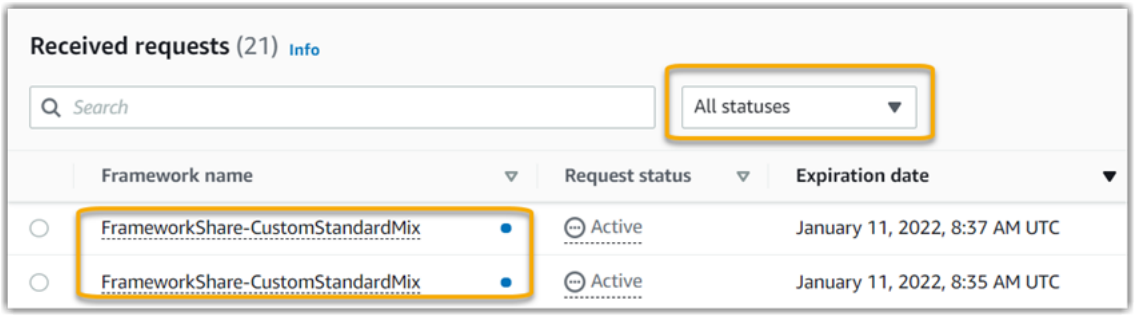
1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Se hai una notifica di richiesta di condivisione, Gestione audit visualizza un punto rosso accanto all'icona del menu di navigazione.

3. Espandi il riquadro di navigazione e guarda accanto a Condividi richieste. Un badge di notifica indica il numero di richieste di condivisione che necessitano della tua attenzione.



4. Scegli Richieste di condivisione. Per impostazione predefinita, questa pagina si apre sulla scheda Richieste ricevute.
5. Identifica le richieste di condivisione che richiedono il tuo intervento cercando gli elementi con un punto blu.



6. (Facoltativo) Per visualizzare solo le richieste in scadenza nei prossimi 30 giorni, trova l'elenco a discesa Tutti gli stati e seleziona In scadenza.

Fase 2: Intervenire sulla richiesta

Per rimuovere il punto blu di notifica, devi intervenire accettando o rifiutando la richiesta di condivisione.

Accettare un framework condiviso

Quando accetti una richiesta di condivisione, Gestione audit replica un'istantanea del framework originale nella scheda framework personalizzati della libreria del framework. Gestione audit replica e crittografa il nuovo framework personalizzato utilizzando la chiave KMS specificata nelle impostazioni di Gestione audit.

Per accettare una richiesta di condivisione

1. Apri la pagina delle Richieste di condivisione e assicurati di visualizzare la scheda Richieste ricevute.
2. (Facoltativo) Seleziona Attive o In scadenza dall'elenco a discesa dei filtri.
3. (Facoltativo) Scegli un nome di framework per visualizzare i dettagli della richiesta di condivisione. Ciò include informazioni come la descrizione del framework, il numero di controlli presenti nel framework e il messaggio del mittente.
4. Seleziona la richiesta di condivisione che desideri accettare, scegli Azioni, quindi scegli Accetta.

Dopo aver accettato una richiesta di condivisione, lo stato passa a Replica mentre il framework personalizzato condiviso viene aggiunto alla libreria del framework. Se il framework contiene controlli personalizzati, questi controlli vengono aggiunti alla libreria di controlli in questo momento.

Al termine della replica del framework, lo stato passa a condiviso. Un banner di successo segnala che il framework personalizzato è pronto per l'uso.

> **Tip**
>
> Quando accetti un framework personalizzato, questo viene replicato solo nella tua Regione AWS attuale. Puoi anche avere il tuo nuovo framework condiviso disponibile in tutte le regioni del tuo Account AWS. In tal caso, dopo aver accettato la richiesta di condivisione, puoi condividere il framework con altre regioni del tuo account, se necessario.

Rifiutare un framework condiviso

Quando rifiuti una richiesta di condivisione, Gestione audit non aggiunge quel framework personalizzato alla tua libreria di framework. Tuttavia, nella scheda Richieste ricevute rimane un record della richiesta di condivisione rifiutata, con lo stato Inattive.

Per rifiutare una richiesta di condivisione

1. Apri la pagina delle Richieste di condivisione e assicurati di visualizzare la scheda Richieste ricevute.
2. (Facoltativo) Seleziona Attive o In scadenza dall'elenco a discesa dei filtri.

3. (Facoltativo) Scegli un nome di framework per visualizzare i dettagli della richiesta di condivisione. Ciò include informazioni come la descrizione del framework, il numero di controlli presenti nel framework e il messaggio del mittente.
4. Seleziona la richiesta di condivisione che desideri rifiutare, scegli Azioni, quindi scegli Rifiuta.
5. Nella finestra di dialogo visualizzata, scegli Rifiuta per confermare la scelta.

> **Tip**
>
> Se cambi idea e desideri accedere a un framework condiviso dopo aver rifiutato, chiedi al mittente di inviarti una nuova richiesta di condivisione.

> **Note**
>
> Possono essere necessari fino a 10 minuti per elaborare le azioni di richiesta di condivisione durante la condivisione di un framework tra Regioni AWS. Dopo essere intervenuto su una richiesta di condivisione tra aree geografiche, ti consigliamo di ricontrollare in un secondo momento per confermare che la richiesta di condivisione è stata accettata o rifiutata correttamente.

Fase 3: visualizzazione di una cronologia delle richieste ricevute

Dopo aver accettato o rifiutato un framework condiviso, puoi tornare alla pagina delle Richieste di condivisione per visualizzare la cronologia delle richieste di condivisione. Puoi filtrare questo elenco in base alle tue esigenze. Ad esempio, puoi applicare filtri per visualizzare solo le richieste che hai accettato.

Per visualizzare una cronologia delle tue richieste di condivisione

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione di sinistra, scegli Richieste di condivisione.
3. Scegli la scheda Richieste ricevute.
4. Trova l'elenco a discesa Tutti gli stati e seleziona uno dei seguenti filtri:

Nome	Descrizione
Active (Attivo)	Questo filtro mostra le richieste di condivisione che non hai ancora accettato o rifiutato.
In scadenza	Questo filtro mostra le richieste di condivisione che scadono nei prossimi 30 giorni.
Condiviso	Questo filtro mostra le richieste di condivisione che hai accettato . Il framework condiviso è ora disponibile nella tua libreria di framework.
Inattivo	Questo filtro mostra le richieste di condivisione che sono state rifiutate o scadute.
Failed (Non riuscito)	Questo filtro mostra le richieste di condivisione che non sono state inviate correttamente. Scegli la parola Non riuscito per visualizzare ulteriori dettagli.

Passaggi successivi

Dopo aver accettato un framework personalizzato condiviso, puoi trovarlo nella scheda framework personalizzati della libreria del framework. Ora puoi usare quel framework per creare una valutazione. Per ulteriori informazioni, consulta Creazione di una valutazione in AWS Audit Manager.

Per istruzioni su come modificare il nuovo framework personalizzato, consultaModifica di un framework personalizzato in AWS Audit Manager.

Risorse aggiuntive

Per trovare soluzioni ai problemi che potresti riscontrare, consultaRisoluzione dei problemi relativi al framework.

Eliminazione delle richieste di condivisione in AWS Audit Manager

Quando non è più necessaria una richiesta di condivisione, è possibile eliminarla dal proprio ambiente Audit Manager. Ciò consente di ripulire l'area di lavoro e concentrarsi sulle richieste pertinenti alle attività e alle priorità attuali.

Quando elimini una richiesta di condivisione, viene eliminata solo la richiesta. Il framework condiviso rimane nella libreria del framework.

Prerequisiti

La procedura seguente presuppone che l'utente abbia già inviato o ricevuto una richiesta di condivisione. Non è possibile eliminare le richieste di condivisione con stato attive o in fase di replica.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per eliminare una richiesta di condivisione in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Per eliminare una richiesta di condivisione

1. Nel riquadro di navigazione, scegli Richieste di condivisione.
2. Scegli la scheda Richieste inviate o Richieste ricevute.
3. Seleziona il framework che non desideri più e scegli Elimina.
4. Nella finestra pop-up che appare, scegli Elimina.

Risorse aggiuntive

Per trovare soluzioni ai problemi che potresti riscontrare, consultaRisoluzione dei problemi relativi al framework.

Eliminazione di un framework personalizzato in AWS Audit Manager

Quando non è più necessario un framework personalizzato, è possibile eliminarlo dal proprio ambiente Audit Manager. Ciò consente di ripulire lo spazio di lavoro e concentrarsi sui framework personalizzati pertinenti alle attività e alle priorità attuali.

Prerequisiti

La procedura seguente presuppone che sia stato precedentemente creato un framework personalizzato.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per eliminare un framework personalizzato in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile eliminare framework personalizzati utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface ()AWS CLI.

> **Note**
>
> L'eliminazione di un framework personalizzato non influisce sulle valutazioni esistenti create dal framework prima della sua eliminazione.

Audit Manager console

Per eliminare un framework personalizzato sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione a sinistra, scegli Libreria Framework e scegli la scheda Framework personalizzati.
3. Seleziona il framework che si desideri eliminare, scegli Azioni, quindi scegli Elimina.
   - In alternativa, puoi aprire un framework personalizzato e scegliere Azioni, Elimina in alto a destra nella pagina di riepilogo del framework.
4. Nella finestra pop-up, scegli Elimina per confermare l'eliminazione.

AWS CLI

Per eliminare un framework personalizzato in AWS CLI

1. Innanzitutto, identifica il framework personalizzato da eliminare. Per fare ciò, esegui il list-assessment-frameworkscomando e specifica `--framework-type` as`Custom`.

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

La risposta restituisce un elenco di framework personalizzati. Trova il framework personalizzato che desideri eliminare e prendi nota dell'ID del framework.

2. Quindi, esegui il delete-assessment-framework`--framework-id`comando e specifica il framework che desideri eliminare.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Per eliminare un framework personalizzato utilizzando l'API

1. Usa l'ListAssessmentFrameworksoperazione e specifica FrameworkType come. `Custom` Trova la risposta, trova il framework personalizzato che desideri eliminare e prendi nota dell'ID del framework.
2. Utilizzare l'DeleteAssessmentFrameworkoperazione per eliminare il framework. Nella richiesta, utilizza il parametro frameworkId per specificare il framework che desideri eliminare.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nella Guida di riferimento all'AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Risorse aggiuntive

Per informazioni sulla conservazione dei dati in Audit Manager, vedereEliminazione dei dati di Gestione audit.

Utilizzo della libreria di controlli per gestire i controlli in AWS Audit Manager

È possibile accedere e gestire i controlli dalla libreria di controlli in AWS Audit Manager.

Punti chiave

Nella libreria di controlli, i controlli sono organizzati nelle seguenti categorie.

- I controlli comuni raccolgono prove che supportano più standard di conformità sovrapposti. I controlli comuni automatizzati contengono uno o più controlli principali correlati, ciascuno dei quali raccoglie prove di supporto da un gruppo predefinito di fonti di dati. Questo vi offre un modo efficiente per identificare le fonti di AWS dati che corrispondono al vostro portafoglio di requisiti di conformità. Le fonti di dati sottostanti per ogni controllo comune automatizzato sono convalidate e gestite da valutatori certificati del settore nei AWS Security Assurance Services.
- I controlli standard raccolgono prove a sostegno di uno specifico standard di conformità. È possibile visualizzare i dettagli dei controlli standard, ma non modificarli o eliminarli. Tuttavia, puoi creare una copia modificabile di qualsiasi controllo standard per creare un nuovo controllo che soddisfi i tuoi requisiti specifici.
- I controlli personalizzati sono controlli che possiedi e definisci. Quando crei un controllo personalizzato, ti consigliamo di scegliere i controlli comuni che rappresentano i tuoi obiettivi e di utilizzarli come fonte di prova. Di conseguenza, il controllo personalizzato può raccogliere tutte le prove pertinenti a tali controlli comuni. Puoi anche utilizzare i controlli di base come fonte di prove o utilizzare altre fonti che definisci tu stesso. Quando hai finito, aggiungi i controlli personalizzati a un framework personalizzato, quindi crea una valutazione per iniziare a raccogliere prove.

Risorse aggiuntive

Per creare e gestire i controlli in Audit Manager, segui le procedure descritte qui.

- Individuazione dei controlli disponibili in AWS Audit Manager
- Revisione di un controllo in AWS Audit Manager
  - Revisione di un controllo comune

Individuazione dei controlli disponibili in AWS Audit Manager

Puoi trovare tutti i controlli disponibili nella pagina della libreria Control nella console Audit Manager.

Puoi anche visualizzare tutti i controlli disponibili utilizzando l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i controlli. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Audit Manager console

Per visualizzare i controlli disponibili sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli una scheda per sfogliare i controlli disponibili.
   - Scegli Comune per visualizzare i controlli comuni forniti da AWS.
   - Scegli Standard per visualizzare i controlli standard forniti da AWS.
   - Scegli Personalizzato per visualizzare i controlli personalizzati che hai creato.

AWS CLI

Per trovare i controlli comuni in (AWS CLI

Esegui il list-common-controlscomando per visualizzare un elenco di controlli comuni.

```
aws controlcatalog list-common-controls
```

È inoltre possibile utilizzare l'`common-control-filter`attributo opzionale per restituire un elenco di controlli comuni con un obiettivo specifico.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

Per trovare altri tipi di controlli nel AWS CLI

Esegui il comando list-controls e specifica `--control-type` as `CustomStandard`, o. `Core`

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

Per trovare controlli comuni utilizzando l'API

Utilizza l'ListCommonControlsoperazione per visualizzare un elenco di controlli comuni disponibili. È inoltre possibile utilizzare l'`commonControlFilter`attributo opzionale per restituire un elenco di controlli con un obiettivo specifico.

Per trovare altri tipi di controllo utilizzando l'API

Utilizzate l'ListControlsoperazione e specificate ControlType come `CustomStandard`, o. `Core`

Per ulteriori informazioni, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nel riferimento AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Quando sei pronto per esplorare i dettagli di un controllo, segui la procedura riportata di seguito. Revisione di un controllo in AWS Audit Manager Questa pagina ti guiderà attraverso i dettagli del controllo e spiegherà le informazioni in esso contenute.

Dalla pagina della libreria dei controlli, puoi anche creare un controllo personalizzato, modificare un controllo personalizzato o eliminare un controllo personalizzato.

Risorse aggiuntive

Per le soluzioni al controllo dei problemi in Audit Manager, vedereRisoluzione dei problemi relativi ai controlli e ai set di controlli.

Revisione di un controllo in AWS Audit Manager

È possibile esaminare i dettagli di un controllo utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Per iniziare a esaminare un controllo in Audit Manager, segui le procedure descritte qui.

- Revisione di un controllo comune
- Revisione di un controllo di base

- Revisione di un controllo standard
- Revisione di un controllo personalizzato

Revisione di un controllo comune

Quando devi esaminare i dettagli di un controllo, troverai le informazioni organizzate in diverse sezioni nella pagina dei dettagli del controllo. Queste sezioni consentono di accedere e comprendere facilmente le informazioni pertinenti per tale controllo.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i controlli comuni in Audit Manager. Più specificamente, sono necessarie le seguenti autorizzazioni per visualizzare i controlli, gli obiettivi di controllo e i domini di controllo comuni forniti da AWS Control Catalog:

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

Una politica suggerita che concede queste autorizzazioni è. AWSAuditManagerAdministratorAccess

Procedura

È possibile esaminare un controllo comune utilizzando la console Audit Manager, l'API AWS Control Catalog o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare i dettagli di controllo comuni sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli Comune per visualizzare i controlli comuni forniti da AWS.
4. Scegli un nome di controllo comune per visualizzarne i dettagli.
5. Rivedi i dettagli del controllo comune utilizzando le seguenti informazioni come riferimento.

Sezione panoramica

Questa sezione descrive il controllo comune.

Scheda Fonti di evidenza

Questa scheda include le seguenti informazioni:

Nome	Descrizione
Controlli principali	Questi sono i controlli principali che raccolgono prove a sostegno del controllo comune. • Quando si raccolgono prove relative a questo controllo comune, si raccolgono automaticamente le prove relative a tutti i controlli principali elencati qui. Quando ciascuno di questi controlli di base viene implementato con successo, ciò aiuta a dimostrare che stai soddisfacendo i requisiti del controllo comune. • Ogni controllo principale utilizza un raggruppamento predefinito di fonti di dati per raccogliere prove su un. Servizio AWS AWS gestisce queste fonti di dati per te. Ciò significa che vengono aggiornate automaticamente ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati. Scegli un controllo di base per visualizzare le fonti di dati sottostanti.

Scheda dei requisiti correlati

Quando raccogli le prove relative a questo controllo comune, le stesse prove possono aiutarti a dimostrare la conformità ai requisiti dei controlli standard correlati elencati in questa scheda. Scegli un controllo standard per visualizzare ulteriori dettagli.

> **Note**
>
> • Il controllo comune potrebbe fornire prove che dimostrino solo la conformità parziale a un controllo standard. È possibile che siano necessarie ulteriori prove per dimostrare la piena conformità a un controllo standard.

- Al momento, la scheda Requisiti correlati mostra solo i controlli standard correlati. Sebbene un controllo comune possa essere correlato a uno o più controlli personalizzati, tali relazioni non vengono visualizzate in questa scheda.

AWS CLI

Per visualizzare i dettagli dei controlli comuni in AWS CLI

1. Esegui il list-common-controlscomando per visualizzare un elenco dei controlli comuni disponibili. Quando si utilizza questa operazione, è possibile applicare un'opzione `common-control-filter` per visualizzare i controlli comuni che hanno un obiettivo specifico.

```
aws controlcatalog list-common-controls
```

2. Nella risposta, identifica il controllo comune che desideri esaminare e prendi nota dei relativi dettagli.

AWS Control Catalog API

Per visualizzare i dettagli dei controlli comuni utilizzando l'API

1. Utilizza l'ListCommonControlsoperazione per visualizzare un elenco di controlli comuni disponibili. Quando si utilizza questa operazione, è possibile applicare un'opzione `commonControlFilter` per visualizzare un elenco di controlli con un obiettivo specifico.
2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dei relativi dettagli.

Per ulteriori informazioni su queste operazioni API, scegli il link in questa procedura per saperne di più nel AWS Control Catalog API Reference. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Puoi scegliere i controlli comuni che rappresentano i tuoi obiettivi e utilizzarli come elementi costitutivi per creare un controllo personalizzato. Ogni controllo comune automatizzato è mappato a un raggruppamento predefinito di fonti di AWS dati che Audit Manager gestisce per te. Ciò significa che

non devi essere un AWS esperto per sapere quali fonti di dati raccolgono le prove pertinenti ai tuoi obiettivi. Inoltre, non è necessario mantenere personalmente queste mappature delle fonti di dati.

Per istruzioni su come creare un controllo personalizzato che utilizzi controlli comuni come fonte di prove, consulta. Creazione di un controllo personalizzato in AWS Audit Manager

Risorse aggiuntive

- Revisione di un controllo di base
- Revisione di un controllo standard
- Revisione di un controllo personalizzato

Revisione di un controllo di base

È possibile esaminare i dettagli di un controllo principale utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i controlli. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Audit Manager console

Per visualizzare i dettagli di controllo di base sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli Comune per visualizzare i controlli comuni forniti da AWS.
4. Cerca il controllo comune adatto al tuo caso d'uso.
5. Scegli l'icona della visualizzazione ad albero accanto al nome del controllo comune. Questo mostra i controlli principali che supportano il controllo comune.
6. Scegli il nome del controllo principale che desideri esaminare.

7. Rivedi i dettagli del controllo principale utilizzando le seguenti informazioni come riferimento.

Sezione panoramica

Questa sezione descrive il controllo principale ed elenca i tipi di fonti di dati da cui raccoglie le prove.

Scheda Fonti di evidenza

Questa scheda include le seguenti informazioni:

Nome	Descrizione

Fonti di dati	Queste sono le fonti di dati AWS gestite da cui il controllo principale raccoglie le prove. Queste fonti di dati vengono aggiornate automaticamente ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati.
	• Mappatura: la parola chiave specifica utilizzata per raccoglie re prove.
	  • Se il tipo è AWS Config, la mappatura è una AWS Config regola (ad esempio). `SNS_ENCRYPTED_KMS`
	  • Se il tipo è AWS Security Hub, la mappatura è un controllo del Security Hub (ad esempio`EC2.1`).
	  • Se il tipo è una chiamata AWS API, la mappatura è una chiamata API (ad esempio`kms_ListKeys`).
	  • Se il tipo è AWS CloudTrail, la mappatura è un CloudTrail evento (ad esempio`CreateAccessKey`).
	• Tipo: il tipo di fonte di dati da cui provengono le prove.
	  • Se Audit Manager raccoglie le prove, il tipo può essere AWS Security Hub, AWS ConfigAWS CloudTrail, o chiamate AWS API.
	  • Se carichi le tue prove, il tipo è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale.
	• Frequenza: con quale frequenza Audit Manager raccoglie prove per un'origine dati di chiamata AWS API.

Scheda Dettagli

Questa scheda include le seguenti informazioni:

Nome	Descrizione
Istruzioni	Le istruzioni che descrivono come testare e correggere il controllo.
Informazioni sui test	Le procedure di test consigliate.
Piano d'azione	Le azioni consigliate da intraprendere se è necessario ripristin are il controllo.

AWS CLI

Per visualizzare i dettagli del controllo di base nel AWS CLI

1. Segui i passaggi per trovare un controllo. Assicurati di impostarlo `--control-type` come e di applicare eventuali filtri opzionali`Core`, se necessario.

```
aws auditmanager list-controls --control-type Core
```

2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e dell'Amazon Resource Name (ARN).
3. Esegui il comando get-control e specifica. `--control-id` Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta get-control Output nella Guida ai comandi.AWS CLI

4. Per visualizzare i dettagli del tag, esegui il list-tags-for-resourcecomando e specifica. `--resource-arn` Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Per visualizzare i dettagli di controllo di base utilizzando l'API

1. Segui i passaggi per trovare un controllo. Assicurati di impostare ControlType come `Core` e di applicare tutti i filtri opzionali necessari.
2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e dell'Amazon Resource Name (ARN).
3. Usa l'GetControloperazione e specifica il ControlID che hai annotato nel passaggio 2.

   > **Tip**
   >
   > I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta GetControl Response Elements nell'AWS Audit Manager API Reference.

4. Per visualizzare i dettagli dei tag, usa l'ListTagsForResourceoperazione e specifica il resourceArn che hai annotato nel passaggio 2.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti in questa procedura per ulteriori informazioni nella Guida di riferimento all'API.AWS Audit Manager Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Puoi scegliere i controlli principali che rappresentano i tuoi obiettivi e utilizzarli come elementi costitutivi per creare un controllo personalizzato. Ogni controllo principale automatizzato è mappato a un raggruppamento predefinito di fonti di AWS dati che Audit Manager gestisce per te. Ciò significa che non devi essere un AWS esperto per sapere quali fonti di dati raccolgono le prove pertinenti ai tuoi obiettivi. Inoltre, non è necessario mantenere personalmente queste mappature delle fonti di dati.

Per istruzioni su come creare un controllo personalizzato che utilizzi i controlli di base come fonte di prove, consulta. Creazione di un controllo personalizzato in AWS Audit Manager

Risorse aggiuntive

- Revisione di un controllo comune
- Revisione di un controllo standard
- Revisione di un controllo personalizzato

Revisione di un controllo standard

È possibile esaminare i dettagli di un controllo standard utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i controlli. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile esaminare i dettagli di un controllo standard utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare i dettagli di controllo standard sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli Standard per visualizzare i controlli standard forniti da AWS.
4. Scegli un nome di controllo standard per visualizzarne i dettagli.
5. Rivedi i dettagli del controllo standard utilizzando le seguenti informazioni come riferimento.

Sezione panoramica

Questa sezione descrive il controllo standard ed elenca i tipi di fonti di dati che utilizza per raccogliere prove.

Scheda Fonti di evidenza

Questa scheda include le seguenti informazioni:

Nome	Descrizione
Controlli principali	Questi sono i controlli principali che raccolgono prove a sostegno del controllo standard. Ogni controllo principale utilizza un raggruppamento predefini to di fonti di dati per raccogliere prove su un. Servizio AWS Queste fonti di dati sono gestite per te da AWS, e vengono aggiornate automaticamente ogni volta che le normative e gli standard cambiano e vengono identificate nuove fonti di dati. Scegli un controllo di base per visualizzare le fonti di dati sottostanti.

Fonti di dati	Queste sono le altre fonti di dati AWS gestite che raccolgono prove a supporto del controllo standard.
	• Mappatura: la parola chiave specifica utilizzata per raccoglie re prove.
	  • Se il tipo è AWS Config, la mappatura è una AWS Config regola (ad esempio). `SNS_ENCRYPTED_KMS`
	  • Se il tipo è AWS Security Hub, la mappatura è un controllo del Security Hub (ad esempio`EC2.1`).
	  • Se il tipo è una chiamata AWS API, la mappatura è una chiamata API (ad esempio`kms_ListKeys`).
	  • Se il tipo è AWS CloudTrail, la mappatura è un CloudTrail evento (ad esempio`CreateAccessKey`).
	• Tipo: il tipo di fonte di dati da cui provengono le prove.
	  • Se Audit Manager raccoglie le prove, il tipo può essere AWS Security Hub, AWS ConfigAWS CloudTrail, o chiamate AWS API.

Nome	Descrizione
	• Se carichi le tue prove, il tipo è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale. • Frequenza: con quale frequenza Audit Manager raccoglie prove per un'origine dati di chiamata AWS API.

Scheda Dettagli

Questa scheda include le seguenti informazioni:

Nome	Descrizione
Istruzioni	Le istruzioni che descrivono come testare e correggere il controllo.
Informazioni sui test	Le procedure di test consigliate.
Piano d'azione	Le azioni consigliate da intraprendere se è necessario ripristin are il controllo.
Tag	I tag associati al controllo.
Chiave	La chiave del tag (ad esempio, uno standard di conformità, un regolamento o una categoria).
Valore	Il valore del tag.

AWS CLI

Per visualizzare i dettagli di controllo standard in AWS CLI

1. Segui i passaggi per trovare un controllo. Assicurati di impostarlo `--control-type` come e di applicare eventuali filtri opzionali`Standard`, se necessario.

```
aws auditmanager list-controls --control-type Standard
```

2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e dell'Amazon Resource Name (ARN).
3. Esegui il comando get-control e specifica. `--control-id` Nell'esempio seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta get-control Output nella guida di riferimento ai comandi AWS CLI

4. Per visualizzare i dettagli del tag, esegui il list-tags-for-resourcecomando e specifica. `--resource-arn` Nell'esempio seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Per visualizzare i dettagli di controllo standard utilizzando l'API

1. Segui i passaggi per trovare un controllo. Assicurati di impostare ControlType come `Standard` e di applicare tutti i filtri opzionali necessari.
2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e dell'Amazon Resource Name (ARN).
3. Usa l'GetControloperazione e specifica il ControlID che hai annotato nel passaggio 2.

> **Tip**
>
> I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta GetControl Response Elements nell'AWS Audit Manager API Reference.

4. Per visualizzare i dettagli dei tag, usa l'ListTagsForResourceoperazione e specifica il resourceArn che hai annotato nel passaggio 2.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti in questa procedura per ulteriori informazioni nella Guida di riferimento all'API.AWS Audit Manager Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Puoi aggiungere un controllo standard a qualsiasi framework personalizzato. Per istruzioni, consulta Creazione di un framework personalizzato in AWS Audit Manager.

Puoi anche personalizzare qualsiasi controllo standard in modo che soddisfi le tue esigenze. Per istruzioni, consulta Creazione di una copia modificabile di un controllo in AWS Audit Manager.

Risorse aggiuntive

- Revisione di un controllo comune
- Revisione di un controllo di base
- Revisione di un controllo personalizzato

Revisione di un controllo personalizzato

È possibile esaminare i dettagli di un controllo personalizzato utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per visualizzare i controlli. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile esaminare i dettagli di un controllo personalizzato utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare i dettagli di controllo personalizzati sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli Personalizzato per visualizzare i controlli personalizzati che hai creato.
4. Scegli un nome di controllo personalizzato per visualizzarne i dettagli.
5. Rivedi i dettagli del controllo personalizzato utilizzando le seguenti informazioni come riferimento.

Sezione panoramica

Questa sezione descrive il controllo personalizzato ed elenca i tipi di fonti di dati che utilizza per raccogliere prove. Fornisce inoltre informazioni su quando il controllo è stato creato e aggiornato l'ultima volta.

Scheda Fonti di evidenza

Questa scheda mostra da dove il controllo personalizzato raccoglie le prove. Include le seguenti informazioni:

Nome	Descrizione
Controlli comuni	Questi sono i controlli comuni che raccolgono prove a supporto del controllo personalizzato. I controlli comuni raccolgono prove utilizzando fonti di dati sottostanti che AWS gestiscono per te. Per ogni controllo comune elencato, Audit Manager raccoglie le prove pertinenti per tutti i controlli principali di supporto. Scegli un controllo comune per visualizzare i controlli principali correlati.
Controlli principali	Questi sono i controlli principali che raccolgono prove a supporto del controllo personalizzato.

Nome	Descrizione
	I controlli principali raccolgono prove utilizzando un gruppo predefinito di fonti di dati che AWS gestiscono per te. Scegli un controllo di base per visualizzare le fonti di dati sottostanti.

Fonti di dati	Queste sono le fonti di dati che raccolgono prove a supporto del controllo personalizzato.
	
	Note
	Queste fonti di dati non sono gestite per te da AWS. Sei responsabile della loro manutenzione.
	
	• Nome: il nome della fonte di dati.
	• Tipo: il tipo di fonte di dati da cui provengono le prove.
	  • Se Audit Manager raccoglie le prove, il tipo può essere AWS Security Hub, AWS ConfigAWS CloudTrail, o chiamate AWS API.
	  • Se carichi le tue prove, il tipo è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale.
	• Mappatura: la parola chiave specifica utilizzata per raccoglie re prove.
	  • Se il tipo è AWS Config, la mappatura è una AWS Config regola (ad esempio). `SNS_ENCRYPTED_KMS`
	  • Se il tipo è AWS Security Hub, la mappatura è un controllo del Security Hub (ad esempio`EC2.1`).
	  • Se il tipo è una chiamata AWS API, la mappatura è una chiamata API (ad esempio`kms_ListKeys`).
	  • Se il tipo è AWS CloudTrail, la mappatura è un CloudTrail evento (ad esempio`CreateAccessKey`).
	• Frequenza: con quale frequenza Audit Manager raccoglie prove per un'origine dati di chiamata AWS API.

Scheda Dettagli

Questa scheda include le seguenti informazioni:

Nome	Descrizione
Istruzioni	Le istruzioni che descrivono come testare e correggere il controllo.
Informazioni sui test	Le procedure di test consigliate.
Piano d'azione	Le azioni consigliate da intraprendere se è necessario ripristin are il controllo.
Tag	I tag associati al controllo.
Chiave	La chiave del tag (ad esempio, uno standard di conformità, un regolamento o una categoria).
Valore	Il valore del tag.

AWS CLI

Per visualizzare i dettagli dei controlli personalizzati in AWS CLI

1. Segui i passaggi per trovare un controllo. Assicurati di impostarlo `--control-type` come e di applicare eventuali filtri opzionali`Custom`, se necessario.

```
aws auditmanager list-controls --control-type Custom
```

2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e dell'Amazon Resource Name (ARN).
3. Esegui il comando get-control e specifica. `--control-id` Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta get-control Output nella Guida ai comandi.AWS CLI

4. Per visualizzare i tag di un controllo, usa il list-tags-for-resourcecomando e specifica. `--resource-arn` Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Per visualizzare i dettagli dei controlli personalizzati utilizzando l'API

1. Segui i passaggi per trovare un controllo. Assicurati di impostare ControlType come `Custom` e di applicare tutti i filtri opzionali necessari.
2. Nella risposta, identifica il controllo che desideri esaminare e prendi nota dell'ID di controllo e del relativo Amazon Resource Name (ARN).
3. Usa l'GetControloperazione e specifica il ControlID che hai annotato nel passaggio 2.

> **Tip**
>
> I dettagli di controllo vengono restituiti in formato JSON. Per aiutarti a comprendere questi dati, consulta GetControl Response Elements nell'AWS Audit Manager API Reference.

4. Per visualizzare i tag per il controllo, utilizzare l'ListTagsForResourceoperazione e specificare il controllo ResourceArn annotato nel passaggio 2.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti di questa procedura per ulteriori informazioni nella Guida di riferimento alle API.AWS Audit Manager Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Puoi aggiungere un controllo personalizzato a qualsiasi framework personalizzato. Per istruzioni, consulta Creazione di un framework personalizzato in AWS Audit Manager.

Puoi anche modificare un controllo personalizzato, creare una copia modificabile di un controllo personalizzato o eliminare un controllo personalizzato che non ti serve più.

Risorse aggiuntive

- Revisione di un controllo comune
- Revisione di un controllo di base
- Revisione di un controllo standard

Creazione di un controllo personalizzato in AWS Audit Manager

Puoi utilizzare controlli personalizzati per raccogliere prove relative alle tue esigenze di conformità specifiche.

Proprio come i controlli standard, i controlli personalizzati raccolgono prove in modo continuo quando sono attivi nelle valutazioni. Puoi anche aggiungere prove manuali a qualsiasi controllo personalizzato che crei. Ogni prova diventa un record che ti aiuta a dimostrare la conformità ai requisiti del controllo personalizzato.

Per iniziare, di seguito sono illustrati alcuni esempi di come è possibile utilizzare i controlli personalizzati:

Mappa i controlli aziendali su raggruppamenti predefiniti di fonti di dati AWS

> È possibile integrare i controlli aziendali in Audit Manager utilizzando controlli comuni come fonte di prove. Scegliete i controlli comuni che rappresentano i vostri obiettivi e utilizzateli come elementi costitutivi per creare un controllo che raccolga le prove relative alle vostre esigenze di conformità. Ogni controllo comune automatizzato è mappato a un raggruppamento predefinito di fonti di dati. Ciò significa che non devi essere un AWS esperto per sapere quali fonti di dati raccolgono le prove pertinenti ai tuoi obiettivi. E quando si utilizzano controlli comuni come fonte di prove, non è più necessario mantenere le mappature delle fonti di dati, perché Audit Manager si occupa di tutto questo per voi.

Crea una domanda di valutazione del rischio del fornitore

Puoi utilizzare controlli personalizzati per supportare il modo in cui gestisci le valutazioni del rischio dei fornitori. Ogni controllo che crei può rappresentare una singola domanda di valutazione del rischio. Ad esempio, il nome del controllo può essere una domanda e puoi fornire una risposta caricando un file o inserendo una risposta testuale come prova manuale.

Punti chiave

Quando si tratta di creare controlli personalizzati in Audit Manager, è possibile scegliere tra due metodi:

1. Creazione di un controllo da zero: questo metodo offre la massima flessibilità e consente di personalizzare il controllo in base alle specifiche esigenze. Questa è una buona opzione quando si ha un requisito di conformità specifico che non è adeguatamente coperto da un controllo esistente. Questo metodo è particolarmente utile quando è necessario mappare i controlli aziendali dell'organizzazione a raggruppamenti predefiniti di fonti di AWS dati o quando si desidera creare domande di valutazione del rischio dei fornitori come controlli individuali.
2. Creazione di una copia modificabile di un controllo esistente: se un controllo standard o personalizzato esistente soddisfa parzialmente le esigenze, è possibile creare una copia modificabile di tale controllo. Questo approccio è più efficiente se è necessario apportare solo modifiche minori a un controllo esistente. Questa è una buona opzione se si desidera modificare alcuni attributi per allineare meglio il controllo ai requisiti specifici. Ad esempio, è possibile modificare la frequenza con cui un controllo utilizza una chiamata API per raccogliere prove e quindi modificare il nome del controllo in base a ciò.

Risorse aggiuntive

Per istruzioni su come creare un controllo personalizzato, consulta le seguenti risorse.

- Creare un controllo personalizzato partendo da zero in AWS Audit Manager
- Creazione di una copia modificabile di un controllo in AWS Audit Manager

Creare un controllo personalizzato partendo da zero in AWS Audit Manager

Quando i requisiti di conformità dell'organizzazione non sono in linea con i controlli standard predefiniti disponibili in AWS Audit Manager, è possibile creare un controllo personalizzato partendo da zero.

Questa pagina descrive i passaggi per creare un controllo personalizzato su misura per le tue esigenze specifiche.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per creare un controllo personalizzato in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Per raccogliere con successo prove da AWS Config e Security Hub, assicurati di fare quanto segue:

- Attivare AWS Config, quindi applicare le impostazioni richieste per l'utilizzo AWS Config con Audit Manager
- Abilita Security Hub, quindi applica le impostazioni richieste per l'utilizzo di Security Hub con Audit Manager

Audit Manager può quindi raccogliere prove ogni volta che viene effettuata una valutazione per una determinata AWS Config regola o per il controllo del Security Hub.

Procedura

Attività

- Fase 1: specifica dei dettagli di controllo
- Fase 2: Specificare le fonti di prova
- Fase 3 (opzionale): Definizione del piano d'azione
- Fase 4: Revisione e creazione del controllo

Fase 1: specifica dei dettagli di controllo

Inizia specificando i dettagli di controllo personalizzato.

> **Important**
>
> Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come Control details o Testing information. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per specificare i dettagli di controllo

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione, scegli libreria di controllo, quindi scegli Crea controllo personalizzato.
3. In Dettagli di controllo, inserisci le seguenti informazioni sul controllo.
   - Controllo: inserisci un nome descrittivo, un titolo o una domanda di valutazione del rischio. Questo valore consente di identificare il controllo nella libreria dei controlli.
   - Descrizione (facoltativo): inserisci i dettagli per aiutare gli altri a comprendere l'obiettivo di controllo. Questa descrizione viene visualizzata nella pagina dei dettagli di controllo.
4. In Informazioni sul test, inserisci i passaggi consigliati per testare il controllo.
5. In Tag, scegli Aggiungi nuovo tag per associare un tag al controllo. Puoi specificare una chiave per ogni tag che meglio descrive il framework di conformità supportato da questo controllo. La chiave tag è obbligatoria e può essere utilizzata come criterio di ricerca quando si cerca questo controllo nella libreria di controllo.
6. Seleziona Successivo.

Fase 2: Specificare le fonti di prova

Quindi, specifica alcune fonti di prova. Una fonte di prove determina da dove il controllo personalizzato raccoglie le prove. È possibile utilizzare fonti AWS gestite, fonti gestite dal cliente o entrambe.

> **Tip**
>
> Ti consigliamo di utilizzare fonti AWS gestite. Ogni volta che una fonte AWS gestita viene aggiornata, gli stessi aggiornamenti vengono applicati automaticamente a tutti i controlli

personalizzati che utilizzano tali fonti. Ciò significa che i controlli personalizzati raccolgono prove in base alle definizioni più recenti di quella fonte di prove.

Se non sei sicuro delle opzioni da scegliere, consulta i seguenti esempi e i nostri consigli.

Il tuo ruolo	Il tuo obiettivo	Fonte di prova consigliata
Professionista GRC	Voglio raccogliere prove per un particolare dominio o obiettivo	AWS gestito (common control) Utilizza un raggruppamento predefinito di fonti di dati mappate a uno specifico controllo comune.
Esperto tecnico	Voglio raccogliere prove sulle AWS risorse di cui sono responsabile	AWS gestito (core control) Utilizza un raggruppamento predefinito di fonti di dati corrispondenti a un AWS requi sito.
Esperto tecnico	Voglio usare una AWS Config regola personalizzata per raccogliere prove	Gestito dal cliente (automati zzatodata source) Utilizza un'origine dati personalizzata per raccogliere prove automatiche specifiche.
Professionista GRC	Voglio raccogliere prove, come documenti e risposte testuali	Gestito dal cliente (manualedata source) Utilizza una fonte di dati personalizzata per caricare le tue prove manuali.

Per specificare un'origine AWS gestita (consigliato)

Ti consigliamo di iniziare scegliendo uno o più controlli comuni. Quando scegli il controllo comune che rappresenta il tuo obiettivo, Audit Manager raccoglie le prove pertinenti per tutti i controlli principali di supporto. Puoi anche scegliere controlli di base individuali se desideri raccogliere prove mirate sul tuo AWS ambiente.

Per specificare una fonte AWS gestita

1. Vai alla sezione delle fonti AWS gestite della pagina.
2. Per aggiungere un controllo comune, segui questi passaggi:
    a. Seleziona Usa un controllo comune che corrisponda al tuo obiettivo di conformità.
    b. Scegli un controllo comune dall'elenco a discesa.
    c. (Facoltativo) Ripetere il passaggio 2 se necessario. È possibile aggiungere fino a cinque controlli comuni.
3. Per rimuovere un controllo comune, scegli la X accanto al nome del controllo.
4. Per aggiungere un controllo principale, procedi nel seguente modo:
    a. Seleziona Usa un controllo di base che corrisponda a una linea guida prescrittiva. AWS
    b. Scegli un controllo comune dall'elenco a discesa.
    c. (Facoltativo) Ripetere il passaggio 4 se necessario. È possibile aggiungere fino a 50 controlli principali.
5. Per rimuovere un controllo principale, scegli la X accanto al nome del controllo.
6. Per aggiungere fonti di dati gestite dal cliente, utilizzate la procedura seguente. Altrimenti, scegli Next (Successivo).

Per specificare un'origine gestita dal cliente

Per raccogliere prove automatiche da un'origine dati, devi scegliere un tipo di origine dati e una mappatura dell'origine dati. Questi dettagli si riferiscono al tuo AWS utilizzo e indicano all'Audit Manager da dove raccogliere le prove. Se desideri fornire le tue prove, sceglierai invece una fonte di dati manuale.

> **Note**
>
> Sei responsabile della manutenzione delle mappature delle fonti di dati che crei in questo passaggio.

Per specificare una fonte gestita dal cliente

1. Vai alla sezione Fonti gestite dai clienti della pagina.
2. Seleziona Usa una fonte di dati per raccogliere prove manuali o automatizzate.
3. Scegli Aggiungi.
4. Selezionare una delle seguenti opzioni:
   - Scegli le chiamate AWS API, quindi scegli una chiamata API e una frequenza di raccolta delle prove.
   - Scegli AWS CloudTrail l'evento, quindi scegli il nome dell'evento.
   - Scegli una regola AWS Config gestita, quindi scegli un identificatore di regola.
   - Scegli una regola AWS Config personalizzata, quindi scegli un identificatore di regola.
   - Scegli AWS Security Hub controllo, quindi scegli un controllo Security Hub.
   - Scegli Origine dati manuale, quindi scegli un'opzione:
     - Caricamento di file: utilizza questa opzione se il controllo richiede la documentazione come prova.
     - Risposta testuale: utilizzate questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.

   > **Tip**
   >
   > Per informazioni sui tipi di origini dati automatizzate e sui suggerimenti per la risoluzione dei problemi, consultaTipi di fonti di dati supportati per prove automatizzate.
   > Se hai bisogno di convalidare la configurazione della tua origine dati con un esperto, scegli per ora l'opzione Origine dati manuale. In tal modo, puoi creare il controllo e aggiungerlo subito a un framework, quindi modificare il controllo in base alle esigenze in un secondo momento.
5. In Nome dell'origine dati, fornisci un nome descrittivo.

6. (Facoltativo) In Dettagli aggiuntivi, inserisci una descrizione dell'origine dati e una descrizione della risoluzione dei problemi.
7. Scegli Aggiungi origine dati
8. (Facoltativo) Per aggiungere un'altra fonte di dati, scegli Aggiungi e ripeti i passaggi 1-7. Puoi aggiungere fino a 100 fonti di dati.
9. Per rimuovere un'origine dati, selezionala dalla tabella, quindi scegli Rimuovi.
10. Quando hai terminato, seleziona Successivo.

Fase 3 (opzionale): Definizione del piano d'azione

Successivamente, specifica le azioni da intraprendere se è necessario correggere questo controllo.

> **Important**
>
> Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come il piano d'azione. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per definire un piano d'azione

1. In Titolo, inserisci un titolo descrittivo per il piano di azione.
2. In Istruzioni, inserisci istruzioni dettagliate per il piano d'azione.
3. Seleziona Successivo.

Fase 4: Revisione e creazione del controllo

Rivedi le informazioni per il controllo. Per modificare le informazioni relative a una fase, scegli Modifica.

Al termine, scegli Crea controllo personalizzato.

Passaggi successivi

Dopo aver creato un nuovo controllo personalizzato, puoi aggiungerlo a un framework personalizzato. Per ulteriori informazioni, consulta Creazione di un framework personalizzato in AWS Audit Manager e Modifica di un framework personalizzato in AWS Audit Manager.

Dopo aver aggiunto il controllo personalizzato a un framework personalizzato, puoi creare una valutazione e iniziare a raccogliere prove. Per ulteriori informazioni, consulta Creazione di una valutazione in AWS Audit Manager.

Per rivisitare il controllo personalizzato in un secondo momento, consultaIndividuazione dei controlli disponibili in AWS Audit Manager. Puoi seguire questi passaggi per individuare il controllo personalizzato in modo da poterlo visualizzare, modificare o eliminare.

Risorse aggiuntive

Per le soluzioni al controllo dei problemi in Audit Manager, vedereRisoluzione dei problemi relativi ai controlli e ai set di controlli.

Creazione di una copia modificabile di un controllo in AWS Audit Manager

Invece di creare un controllo personalizzato da zero, è possibile utilizzare un controllo standard o un controllo personalizzato esistente come punto di partenza e creare una copia modificabile che soddisfi le proprie esigenze. Quando si esegue questa operazione, il controllo standard esistente rimane nella libreria dei controlli e viene creato un nuovo controllo con le impostazioni personalizzate.

Prerequisiti

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per creare un framework personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Per raccogliere con successo prove da AWS Config e Security Hub, assicurati di fare quanto segue:

- Attivare AWS Config, quindi applicare le impostazioni richieste per l'utilizzo AWS Config con Audit Manager.
- Abilita Security Hub, quindi applica le impostazioni richieste per l'utilizzo di Security Hub con Audit Manager.

Audit Manager può quindi raccogliere prove ogni volta che viene effettuata una valutazione per una determinata AWS Config regola o per il controllo del Security Hub.

Procedura

Attività

- Fase 1: specifica dei dettagli di controllo
- Fase 2: Specificare le fonti di prova
- Fase 3 (Facoltativa): Definizione di un piano di azione
- Fase 4: Revisione e creazione del controllo

Fase 1: specifica dei dettagli di controllo

I dettagli di controllo vengono ereditati dal controllo originale. Esamina e modifica questi dettagli in base alle esigenze.

> **Important**
>
> Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come Control details o Testing information. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per specificare i dettagli di controllo

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Seleziona il controllo standard o il controllo personalizzato a cui desideri apportare modifiche, quindi scegli Crea una copia.
4. Specificate il nuovo nome del controllo e scegliete Continua.
5. In Dettagli di controllo, personalizza i dettagli di controllo in base alle esigenze.
6. In Informazioni sui test, apporta le modifiche necessarie alle istruzioni.
7. In Tag, personalizza i tag in base alle esigenze.
8. Seleziona Successivo.

Fase 2: Specificare le fonti di prova

Le fonti di prova sono ereditate dal controllo originale. È possibile modificare, aggiungere o rimuovere le fonti di prova in base alle esigenze.

Per specificare una fonte AWS gestita (consigliato)

> **Tip**
>
> Ti consigliamo di iniziare scegliendo uno o più controlli comuni. Se hai requisiti di conformità più dettagliati, puoi anche scegliere uno o più controlli di base specifici.

Per specificare una fonte gestita AWS

1. In Fonti AWS gestite, rivedi le selezioni correnti e apporta le modifiche necessarie.
2. Per aggiungere un controllo comune, segui questi passaggi:
   a. Seleziona Usa un controllo comune che corrisponda al tuo obiettivo di conformità.
   b. Scegli un controllo comune dall'elenco a discesa.
   c. (Facoltativo) Ripetere il passaggio 2 se necessario. È possibile aggiungere fino a cinque controlli comuni.
3. Per rimuovere un controllo comune, scegli la X accanto al nome del controllo.
4. Per aggiungere un controllo principale, procedi nel seguente modo:
   a. Seleziona Usa un controllo di base che corrisponda a una linea guida prescrittiva. AWS
   b. Scegli un controllo comune dall'elenco a discesa.
   c. (Facoltativo) Ripetere il passaggio 4 se necessario. È possibile aggiungere fino a 50 controlli principali.
5. Per rimuovere un controllo principale, scegli la X accanto al nome del controllo.
6. Per modificare le fonti di dati gestite dal cliente, utilizzate la procedura seguente. Altrimenti, scegli Next (Successivo).

Per specificare un'origine gestita dal cliente

Per raccogliere prove automatiche da un'origine dati, devi scegliere un tipo di origine dati e una mappatura dell'origine dati. Questi dettagli si riferiscono al tuo AWS utilizzo e indicano all'Audit

Manager da dove raccogliere le prove. Se desideri fornire le tue prove, sceglierai invece una fonte di dati manuale.

> **Note**
>
> Sei responsabile della manutenzione delle mappature delle fonti di dati che crei in questo passaggio.

Per specificare una fonte gestita dal cliente

1. In Fonti gestite dal cliente, esamina le fonti di dati correnti e apporta le modifiche necessarie.
2. Per rimuovere un'origine dati, seleziona un'origine dati dalla tabella e scegli Rimuovi.
3. Per aggiungere una nuova fonte di dati, segui questi passaggi:

    a. Seleziona Usa una fonte di dati per raccogliere prove manuali o automatizzate.
    b. Scegli Aggiungi.
    c. Selezionare una delle seguenti opzioni:

    - Scegli le chiamate AWS API, quindi scegli una chiamata API e una frequenza di raccolta delle prove.
    - Scegli AWS CloudTrail l'evento, quindi scegli il nome dell'evento.
    - Scegli una regola AWS Config gestita, quindi scegli un identificatore di regola.
    - Scegli una regola AWS Config personalizzata, quindi scegli un identificatore di regola.
    - Scegli AWS Security Hub controllo, quindi scegli un controllo Security Hub.
    - Scegli Origine dati manuale, quindi scegli un'opzione:
        - Caricamento di file: utilizza questa opzione se il controllo richiede la documentazione come prova.
        - Risposta testuale: utilizzate questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.

    > **Tip**
    >
    > Per informazioni sui tipi di origini dati automatizzate e sui suggerimenti per la risoluzione dei problemi, consultaTipi di fonti di dati supportati per prove automatizzate.

Se hai bisogno di convalidare la configurazione della tua origine dati con un esperto, scegli per ora l'opzione Origine dati manuale. In tal modo, puoi creare il controllo e aggiungerlo subito a un framework, quindi modificare il controllo in base alle esigenze in un secondo momento.

d. In Nome dell'origine dati, fornisci un nome descrittivo.

e. (Facoltativo) In Dettagli aggiuntivi, inserisci una descrizione dell'origine dati e una descrizione della risoluzione dei problemi.

f. Scegli Aggiungi origine dati

g. (Facoltativo) Per aggiungere un'altra fonte di dati, scegli Aggiungi e ripeti il passaggio 3. Puoi aggiungere fino a 100 fonti di dati.

4. Quando hai terminato, seleziona Successivo.

Fase 3 (Facoltativa): Definizione di un piano di azione

Il piano di azione è ereditato dal controllo originale. È possibile modificare questo piano di azione in base alle esigenze.

Important

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come il piano d'azione. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per specificare le istruzioni

1. In Titolo, rivedi il titolo e apporta le modifiche necessarie.
2. In Istruzioni, rivedi le istruzioni e apporta le modifiche necessarie.
3. Seleziona Successivo.

Fase 4: Revisione e creazione del controllo

Rivedi le informazioni per il controllo. Per modificare le informazioni relative a una fase, scegli Modifica. Al termine, scegli Crea controllo personalizzato.

Passaggi successivi

Dopo aver creato un nuovo controllo personalizzato, puoi aggiungerlo a un framework personalizzato. Per ulteriori informazioni, consulta Creazione di un framework personalizzato in AWS Audit Manager e Modifica di un framework personalizzato in AWS Audit Manager.

Dopo aver aggiunto un controllo personalizzato a un framework personalizzato, puoi creare una valutazione e iniziare a raccogliere prove. Per ulteriori informazioni, consulta Creazione di una valutazione in AWS Audit Manager.

Per rivisitare il controllo personalizzato in un secondo momento, consultaIndividuazione dei controlli disponibili in AWS Audit Manager. Puoi seguire questi passaggi per individuare il controllo personalizzato in modo da poterlo visualizzare, modificare o eliminare.

Risorse aggiuntive

Per le soluzioni al controllo dei problemi in Audit Manager, vedereRisoluzione dei problemi relativi ai controlli e ai set di controlli.

Modifica di un controllo personalizzato in AWS Audit Manager

Potrebbe essere necessario modificare i controlli personalizzati AWS Audit Manager man mano che cambiano i requisiti di conformità.

Questa pagina descrive i passaggi per modificare i dettagli di un controllo personalizzato, le fonti di evidenza e le istruzioni del piano d'azione.

Prerequisiti

La procedura seguente presuppone che sia stato precedentemente creato un controllo personalizzato.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per modificare un controllo personalizzato. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

Segui questi passaggi per modificare un controllo personalizzato.

> **Note**
>
> Quando modifichi un controllo, le modifiche vengono applicate a tutte le valutazioni in cui il controllo è attivo. In tutte queste valutazioni, Audit Manager inizierà automaticamente a raccogliere prove in base alla definizione di controllo più recente.

Attività

- Fase 1: modifica dei dettagli di controllo
- Fase 2: Modifica le fonti di prova
- Fase 3: modifica del piano di azione

Fase 1: modifica dei dettagli di controllo

Rivedi e modifica i dettagli del controllo secondo necessità.

> **Important**
>
> Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come Dettagli di controllo o Informazioni di test. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per modificare i dettagli di controllo

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Libreria di controllo, quindi scegli la scheda Personalizzata.
3. Seleziona il controllo che desideri modificare e scegli Modifica.
4. In Dettagli di controllo, modifica i dettagli di controllo in base alle esigenze.
5. In Informazioni sui test, modifica la descrizione in base alle esigenze.
6. Seleziona Successivo.

Fase 2: Modifica le fonti di prova

Successivamente, puoi modificare, rimuovere o aggiungere fonti di prova per il controllo.

> **Note**
>
> Quando modifichi un controllo per includere più o meno fonti di evidenza, ciò potrebbe influire sulla quantità di prove raccolte dal controllo in tutte le valutazioni in cui è attivo. Ad esempio, se si aggiungono fonti di evidenza, è possibile notare che Audit Manager esegue più valutazioni delle risorse e raccoglie più prove rispetto a prima. Se rimuovi le fonti di prova, è probabile che il tuo controllo raccoglierà meno prove in futuro.
> Per ulteriori informazioni sulla valutazione delle risorse e sui prezzi, consulta AWS Audit Manager Prezzi.

Per modificare una fonte AWS gestita

Per modificare una fonte AWS gestita

1. In Fonti AWS gestite, rivedi le selezioni correnti e apporta le modifiche necessarie.
2. Per aggiungere un controllo comune, segui questi passaggi:
   a. Seleziona Usa un controllo comune che corrisponda al tuo obiettivo di conformità.
   b. Scegli un controllo comune dall'elenco a discesa.
   c. (Facoltativo) Ripetere il passaggio 2 se necessario. È possibile aggiungere fino a cinque controlli comuni.
3. Per rimuovere un controllo comune, scegli la X accanto al nome del controllo.
4. Per aggiungere un controllo principale, procedi nel seguente modo:
   a. Seleziona Usa un controllo di base che corrisponda a una linea guida prescrittiva. AWS
   b. Scegli un controllo comune dall'elenco a discesa.
   c. (Facoltativo) Ripetere il passaggio 4 se necessario. È possibile aggiungere fino a 50 controlli principali.
5. Per rimuovere un controllo principale, scegli la X accanto al nome del controllo.
6. Per aggiungere fonti di dati gestite dal cliente, utilizzate la procedura seguente. Altrimenti, scegli Next (Successivo).

Per modificare una fonte gestita dal cliente

> **Note**
>
> Sei responsabile della manutenzione delle mappature delle fonti di dati che modifichi in questo passaggio.

Per modificare una fonte gestita dal cliente

1. In Fonti gestite dal cliente, esamina le fonti di dati correnti e apporta le modifiche necessarie.
2. Per rimuovere un'origine dati, seleziona un'origine dati dalla tabella, quindi scegli Rimuovi.
3. Per aggiungere una nuova fonte di dati, segui questi passaggi:
   a. Seleziona Usa una fonte di dati per raccogliere prove manuali o automatizzate.
   b. Scegli Aggiungi.
   c. Selezionare una delle seguenti opzioni:
      - Scegli le chiamate AWS API, quindi scegli una chiamata API e una frequenza di raccolta delle prove.
      - Scegli AWS CloudTrail l'evento, quindi scegli il nome dell'evento.
      - Scegli una regola AWS Config gestita, quindi scegli un identificatore di regola.
      - Scegli una regola AWS Config personalizzata, quindi scegli un identificatore di regola.
      - Scegli AWS Security Hub controllo, quindi scegli un controllo Security Hub.
      - Scegli Origine dati manuale, quindi scegli un'opzione:
        - Caricamento di file: utilizza questa opzione se il controllo richiede la documentazione come prova.
        - Risposta testuale: utilizzate questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.

> **Tip**
>
> Per informazioni sui tipi di origini dati automatizzate e sui suggerimenti per la risoluzione dei problemi, consultaTipi di fonti di dati supportati per prove automatizzate.

Se hai bisogno di convalidare la configurazione della tua origine dati con un esperto, scegli per ora l'opzione Origine dati manuale. In tal modo, puoi creare il controllo e aggiungerlo subito a un framework, quindi modificare il controllo in base alle esigenze in un secondo momento.

d. In Nome dell'origine dati, fornisci un nome descrittivo.

e. (Facoltativo) In Dettagli aggiuntivi, inserisci una descrizione dell'origine dati e una descrizione della risoluzione dei problemi.

f. Scegli Aggiungi origine dati

g. (Facoltativo) Per aggiungere un'altra fonte di dati, scegli Aggiungi e ripeti il passaggio 3. Puoi aggiungere fino a 100 fonti di dati.

4. Quando hai terminato, seleziona Successivo.

Fase 3: modifica del piano di azione

Successivamente, rivedi e modifica il piano di azione facoltativo.

Important

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi in formato libero come Action plan. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Per modificare un piano di azione

1. In Titolo, modifica il titolo in base alle esigenze.
2. In Istruzioni, modifica le istruzioni in base alle esigenze.
3. Seleziona Successivo.

Fase 4: Rivedi e salva

Rivedi le informazioni per il controllo. Per modificare le informazioni relative a una fase, scegli Modifica.

Al termine, scegli Salva le modifiche.

> **Note**
>
> Dopo aver modificato un controllo, le modifiche hanno effetto come segue in tutte le valutazioni attive che includono il controllo:
>
> - Per i controlli con Chiamate API AWS come tipo di origine dati, le modifiche hanno effetto alle 00:00 UTC del giorno successivo.
> - Per tutti gli altri controlli, le modifiche diventano effettive immediatamente.

Passaggi successivi

Quando sei sicuro di non aver più bisogno di un controllo personalizzato, puoi ripulire il tuo ambiente Audit Manager eliminando il controllo. Per istruzioni, consulta Eliminazione di un controllo personalizzato in AWS Audit Manager.

Risorse aggiuntive

Per le soluzioni al controllo dei problemi in Audit Manager, vedereRisoluzione dei problemi relativi ai controlli e ai set di controlli.

Modifica della frequenza con cui un controllo raccoglie le prove

AWS Audit Manager può raccogliere prove da varie fonti di dati. La frequenza della raccolta delle prove dipende dal tipo di fonte di dati utilizzata dal controllo.

Le sezioni seguenti forniscono ulteriori informazioni sulla frequenza di raccolta delle prove per ogni tipo di origini dati di controllo e su come modificarla (se applicabile).

Argomenti

Punti chiave

- Per le chiamate API AWS , Gestione audit raccoglie prove utilizzando una chiamata API di descrizione a un'altra Servizio AWS. È possibile specificare la frequenza di raccolta delle prove direttamente in Gestione audit (solo per i controlli personalizzati).
- Perché AWS Config, Audit Manager riporta il risultato di un controllo di conformità direttamente da AWS Config. La frequenza segue i trigger definiti nella AWS Config regola.
- Per AWS Security Hub, Gestione audit riporta il risultato di un controllo di conformità direttamente da Security Hub. La frequenza segue la pianificazione del controllo Security Hub.
- Perché AWS CloudTrail, Audit Manager raccoglie continuamente prove da CloudTrail. Non puoi modificare la frequenza per questo tipo di prova.

Istantanee di configurazione dalle chiamate API AWS

> **Note**
>
> Quanto segue si applica solo ai controlli personalizzati. Non è possibile modificare la frequenza di raccolta delle prove per un controllo standard.

Se un controllo personalizzato utilizza le chiamate AWS API come tipo di origine dati, puoi modificare la frequenza di raccolta delle prove in Audit Manager seguendo questi passaggi.

Per modificare la frequenza di raccolta delle prove per un controllo personalizzato con un'origine dati di chiamata API

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione, scegli Libreria di controllo, quindi scegli la scheda Personalizzata.
3. Seleziona il controllo personalizzato che desideri modificare e scegli Modifica.
4. Nella pagina Modifica dettagli controllo, scegli Avanti.
5. In Fonti gestite dai clienti, cerca l'origine dei dati delle chiamate API che desideri aggiornare.
6. Seleziona l'origine dati dalla tabella, quindi scegli Rimuovi.
7. Scegli Aggiungi.
8. Scegli chiamate AWS API.

9. Scegli la stessa chiamata API che hai rimosso nel passaggio 5, quindi seleziona la frequenza di raccolta delle prove preferita.
10. In Nome dell'origine dati, fornisci un nome descrittivo.
11. (Facoltativo) In Dettagli aggiuntivi, inserisci una descrizione dell'origine dati e una descrizione della risoluzione dei problemi.
12. Seleziona Successivo.
13. Nella pagina Modifica un piano di azione, scegli Avanti.
14. Nella pagina Revisione e aggiornamento, esamina le informazioni per il controllo personalizzato. Per modificare le informazioni relative a una fase, scegli Modifica.
15. Al termine, scegli Salva le modifiche.

Dopo aver modificato un controllo, le modifiche entrano in vigore alle 00:00 UTC del giorno successivo in tutte le valutazioni attive che includono il controllo.

Controlli di conformità da AWS Config

> **Note**
>
> Quanto segue si applica sia ai controlli standard che ai controlli personalizzati che utilizzano Regole di AWS Config come origine dati.

Se un controllo utilizza AWS Config come tipo di origine dati, non è possibile modificare la frequenza di raccolta delle prove direttamente in Audit Manager. Questo perché la frequenza segue i trigger definiti nella AWS Config regola.

Esistono due tipi di trigger per: Regole di AWS Config

1. Modifiche alla configurazione: AWS Config esegue le valutazioni della regola quando determinati tipi di risorse vengono creati, modificati o eliminati.
2. Periodico: AWS Config esegue le valutazioni della regola con una frequenza scelta dall'utente (ad esempio, ogni 24 ore).

Per ulteriori informazioni sui trigger per Regole di AWS Config, consulta Tipi di trigger nella Guida per gli AWS Config sviluppatori.

Per istruzioni su come gestire Regole di AWS Config, consulta Gestire le AWS Config regole.

Controlli di conformità da Security Hub

> **Note**
>
> Quanto segue si applica sia ai controlli standard che ai controlli personalizzati che utilizzano i controlli Security Hub come origine dati.

Se un controllo utilizza Security Hub come tipo di origine dati, non è possibile modificare la frequenza di raccolta delle prove direttamente in Gestione audit. Ciò perché la frequenza segue la pianificazione dei controlli Security Hub.

- I controlli periodici vengono eseguiti automaticamente entro 12 ore dall'ultima esecuzione. Non è possibile modificare la periodicità.
- I Controlli attivati dalle modifiche vengono eseguiti quando la risorsa associata cambia stato. Anche se la risorsa non cambia stato, l'ora dei controlli attivati dalle modifiche viene aggiornata ogni 18 ore. Ciò consente di indicare che il controllo è ancora abilitato. In generale, Security Hub utilizza regole modificate quando possibile.

Per ulteriori informazioni, consulta Pianificazione dell'esecuzione dei controlli di sicurezza nella Guida per l'utente AWS Security Hub .

Registri delle attività degli utenti da AWS CloudTrail

> **Note**
>
> Quanto segue si applica sia ai controlli standard che ai controlli personalizzati che utilizzano i log delle attività dell'utente AWS CloudTrail come origine dati.

Non è possibile modificare la frequenza di raccolta delle prove per i controlli che utilizzano i registri delle attività CloudTrail come tipo di origine dati. Audit Manager raccoglie questo tipo di prove CloudTrail in modo continuo. La frequenza è continua perché l'attività dell'utente può avvenire in qualsiasi momento della giornata.

Eliminazione di un controllo personalizzato in AWS Audit Manager

Se hai creato un controllo personalizzato e non ti serve più, puoi eliminarlo dal tuo ambiente Audit Manager. Ciò consente di ripulire l'area di lavoro e concentrarsi sui controlli personalizzati pertinenti alle attività e alle priorità correnti.

Prerequisiti

La procedura seguente presuppone che sia stato precedentemente creato un controllo personalizzato.

Assicurati che la tua identità IAM disponga delle autorizzazioni appropriate per eliminare un controllo personalizzato in. AWS Audit Manager Due politiche suggerite per concedere queste autorizzazioni sono AWSAuditManagerAdministratorAccesse. Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

Procedura

È possibile eliminare i controlli personalizzati utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Important**
>
> Quando elimini un controllo personalizzato, questa azione rimuove il controllo da tutti i framework o le valutazioni personalizzati a cui è attualmente correlato. Di conseguenza, Gestione audit smetterà di raccogliere prove per quel controllo personalizzato in tutte le tue valutazioni. Ciò include le valutazioni create in precedenza prima di eliminare il controllo personalizzato.

Audit Manager console

Per eliminare un controllo personalizzato dalla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel pannello di navigazione, scegli Libreria di controllo, quindi scegli la scheda Controlli personalizzati.
3. Seleziona il controllo da eliminare, quindi scegli Elimina.
4. Nella finestra pop-up che appare, scegli Elimina per confermare.

AWS CLI

Per eliminare un controllo personalizzato in AWS CLI

1. Innanzitutto, identifica il controllo personalizzato che desideri eliminare. Per fare ciò, esegui il comando list-controls e specifica `--control-type` come `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   La risposta restituisce un elenco di controlli personalizzati. Trova il controllo che desideri eliminare e prendi nota dell'ID di controllo.
2. Quindi, esegui il comando delete-control e usa il parametro `--control-id` per specificare il controllo che desideri eliminare.

   Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Per eliminare un controllo personalizzato utilizzando l'API

1. Utilizzate l'ListControlsoperazione e specificate ControlType come. `Custom` Dalla risposta, individua il controllo che desideri eliminare e annota l'ID del controllo.
2. Utilizzare l'DeleteControloperazione per eliminare il controllo personalizzato. Nella richiesta, utilizza il parametro ControlId per specificare il controllo che desideri eliminare.

Per ulteriori informazioni su queste operazioni API, scegliete uno dei collegamenti nella procedura precedente per ulteriori informazioni nella Guida di riferimento all'AWS Audit Manager API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Risorse aggiuntive

Per informazioni sulla conservazione dei dati in Audit Manager, vedereEliminazione dei dati di Gestione audit.

Revisione e configurazione delle impostazioni AWS Audit Manager

Puoi rivedere e configurare AWS Audit Manager le tue impostazioni in qualsiasi momento per assicurarti che soddisfino le tue esigenze specifiche.

Questo capitolo illustra il processo di accesso, revisione e regolazione delle impostazioni step-by-step di Audit Manager. Seguendo, imparerai come modificare le impostazioni generali, le impostazioni di valutazione e le impostazioni di Evidence Finder per allinearle agli obiettivi di conformità e ai requisiti aziendali in evoluzione.

Procedura

Per iniziare, segui questi passaggi per visualizzare le impostazioni dell'Audit Manager. È possibile visualizzare le impostazioni di Audit Manager utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Per visualizzare le impostazioni

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Scegli la scheda che soddisfa il tuo obiettivo.

   - Impostazioni generali: scegliere questa scheda per rivedere e aggiornare le impostazioni generali di Audit Manager.
   - Impostazioni di valutazione: scegli questa scheda per rivedere e aggiornare le impostazioni predefinite per le tue valutazioni.
   - Impostazioni dello strumento di ricerca delle prove: scegli questa scheda per rivedere e aggiornare le impostazioni dello strumento di ricerca delle prove.

Passaggi successivi

Per personalizzare le impostazioni di Audit Manager per il tuo caso d'uso, segui le procedure descritte qui.

- Impostazioni generali
  - Configurazione delle impostazioni di crittografia dei dati
  - Aggiungere un amministratore delegato
  - Modifica di un amministratore delegato
  - Rimozione di un amministratore delegato
  - Disabilitazione AWS Audit Manager
- Impostazioni di valutazione
  - Configurazione dei proprietari di audit predefiniti
  - Configurazione della destinazione predefinita del rapporto di valutazione
  - Configurazione delle notifiche di Audit Manager
- Impostazioni Evidence Finder
  - Attivazione di evidence finder
  - Conferma dello stato di Evidence Finder
  - Configurazione della destinazione di esportazione predefinita per Evidence Finder
  - Disabilitare evidence finder

Configurazione delle impostazioni di crittografia dei dati

Puoi scegliere come crittografare i tuoi dati. AWS Audit Manager Audit Manager crea automaticamente un Chiave gestita da AWS file unico per l'archiviazione sicura dei dati. Per impostazione predefinita, i dati di Gestione audit sono crittografati con questa chiave KMS. Tuttavia, se desideri personalizzare le impostazioni di crittografia dei dati, puoi specificare la tua chiave di crittografia simmetrica gestita dal cliente. L'utilizzo di una propria Chiave KMS offre una maggiore flessibilità che include la possibilità di creare, ruotare e disabilitare le chiavi.

Prerequisiti

Se fornisci una chiave gestita dal cliente, questa deve corrispondere alla tua valutazione per generare report di valutazione ed esportare correttamente i risultati della ricerca di Evidence Finder. Regione AWS

Procedura

È possibile aggiornare le impostazioni di crittografia dei dati utilizzando la console Gestione audit, AWS Command Line Interface (AWS CLI) o l'API Gestione audit.

> **Note**
>
> Quando modifichi le impostazioni di crittografia dei dati di Gestione audit, queste modifiche si applicano a tutte le nuove valutazioni che crei. Ciò include tutti i report di valutazione e le esportazioni di Evidence finder che crei a partire dalle nuove valutazioni.
> Le modifiche non si applicano alle valutazioni esistenti che hai creato prima di modificare le impostazioni di crittografia. Ciò include nuovi rapporti di valutazione ed esportazioni CSV creati a partire da valutazioni esistenti, oltre ai report di valutazione e alle esportazioni CSV esistenti. Le valutazioni esistenti, con tutti i relativi rapporti di valutazione ed esportazioni in formato CSV, continuano a utilizzare la vecchia chiave KMS. Se l'identità IAM che genera il rapporto di valutazione non può utilizzare la vecchia chiave KMS, concedi le autorizzazioni policy della chiave.

Audit Manager console

Per aggiornare le impostazioni di crittografia dei dati sulla console Audit Manager

1. Dalla scheda Impostazioni generali, vai alla sezione Crittografia dei dati.
2. Per utilizzare la chiave KMS predefinita fornita da Gestione audit, deselezionare la casella di controllo Personalizza le impostazioni di crittografia (avanzate).
3. Per utilizzare una chiave gestita dal cliente, selezionare la casella di controllo Personalizza le impostazioni di crittografia (avanzate). Puoi selezionare una coppia di chiavi esistente o crearne una nuova.

AWS CLI

Per aggiornare le impostazioni di crittografia dei dati in AWS CLI

Esegui il comando update-settings e utilizza il parametro `--kms-key` per specificare la tua chiave gestita dal cliente.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Per aggiornare le impostazioni di crittografia dei dati utilizzando l'API

Chiama l'UpdateSettingsoperazione e utilizza il parametro KMSKey per specificare la tua chiave gestita dal cliente.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Risorse aggiuntive

- Per istruzioni sulla creazione di chiavi, consulta Creazione di chiavi nella Guida per l'utente AWS Key Management Service .
- Per istruzioni su come concedere le autorizzazioni a livello di policy chiave, consulta Consentire agli utenti di altri account di utilizzare una chiave KMS nella Guida per gli sviluppatori. AWS Key Management Service

Aggiungere un amministratore delegato

Se utilizzi AWS Organizations e desideri abilitare il supporto multi-account per AWS Audit Manager, puoi designare un account membro della tua organizzazione come amministratore delegato per Audit Manager.

Se si desidera utilizzare Audit Manager in più di una regione Regione AWS, è necessario designare un account amministratore delegato separatamente in ciascuna regione. Nelle impostazioni di Gestione audit, è necessario utilizzare lo stesso account amministratore delegato in tutte le regioni.

Prerequisiti

Prendi nota dei seguenti fattori che definiscono il modo in cui l'amministratore delegato opera in Gestione audit:

- L'account deve essere un membro di un'Organizzazione .
- Prima di designare un amministratore delegato, è necessario abilitare tutte le funzionalità dell'organizzazione. È inoltre necessario configurare le impostazioni del Security Hub

dell'organizzazione. In tal modo, Gestione audit può raccogliere le prove del Security Hub dagli account dei tuoi membri.

- L'account amministratore delegato deve avere accesso alla chiave KMS fornita durante la configurazione di Gestione audit.
- Non puoi utilizzare il tuo account di AWS Organizations gestione come amministratore delegato in Audit Manager.

Procedura

È possibile aggiungere un amministratore delegato utilizzando la console Gestione audit, AWS Command Line Interface (AWS CLI) o l'API Gestione audit.

> **Note**
>
> Dopo aver aggiunto un amministratore delegato nelle impostazioni di Gestione audit, l'account di gestione non può più creare valutazioni aggiuntive in Gestione audit. Inoltre, la raccolta delle prove si interrompe per tutte le valutazioni esistenti create dall'account di gestione. Gestione audit raccoglie e allega prove all'account amministratore delegato, che è l'account principale per la gestione delle valutazioni dell'organizzazione.

Audit Manager console

Per aggiungere un amministratore delegato sulla console Audit Manager

1. Dalla scheda impostazioni Generali, vai alla sezione Amministratore delegato.
2. In ID account amministratore delegato, inserisci l'ID dell'account dell'amministratore delegato.
3. Scegli Delega.

AWS CLI

Per aggiungere un amministratore delegato nel AWS CLI

Eseguire il register-organization-admin-accountcomando e utilizzare il `--admin-account-id` parametro per specificare l'ID account dell'amministratore delegato.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Per aggiungere un amministratore delegato utilizzando l'API

Chiama l'RegisterOrganizationAdminAccountoperazione e utilizza il adminAccountIdparametro per specificare l'ID account dell'amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Per modificare l'account di amministratore delegato, consulta. Modifica di un amministratore delegato

Per rimuovere il tuo account di amministratore delegato, consulta. Rimozione di un amministratore delegato

Risorse aggiuntive

- Creazione e gestione di un'organizzazione
- Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations

Modifica di un amministratore delegato

La modifica dell'amministratore delegato AWS Audit Manager è una procedura in due fasi. Innanzitutto, devi rimuovere l'attuale account di amministratore delegato. Quindi, puoi aggiungere un nuovo account come amministratore delegato.

Segui i passaggi in questa pagina per modificare l'amministratore delegato.

Indice

- Procedura
- Passaggi successivi
- Risorse aggiuntive

Prerequisiti

Prima di rimuovere l'account corrente

Prima di rimuovere l'attuale account di amministratore delegato, tieni presenti le seguenti considerazioni:

- Attività di pulizia delle evidenze: se l'attuale amministratore delegato (account A) ha abilitato Evidence Finder, dovrai eseguire un'attività di pulizia prima di assegnare l'account B come nuovo amministratore delegato.

  Prima di utilizzare l'account di gestione per rimuovere l'account A, assicurati che l'account A acceda a Audit Manager e disattivi lo strumento di ricerca delle prove. Disabilitare evidence finder comporta l'eliminazione automatica di un l'archivio di dati degli eventi creato nell'account quando evidence finder era abilitato.

  Se questa attività non viene completata, l'archivio dati degli eventi rimane nell'account A. In questo caso, consigliamo che l'amministratore delegato originale utilizzi CloudTrail Lake per eliminare manualmente l'Event Data Store.

  Questa attività di pulizia è necessaria per assicurarti che non ti ritroverai con più archivi di dati degli eventi. Dopo la rimozione o la modifica di un account amministratore delegato, Gestione audit ignora un archivio di dati degli eventi non utilizzato. Tuttavia, se non elimini l'Event Data Store inutilizzato, l'Event Data Store continua a comportare costi di archiviazione da parte di Lake. CloudTrail
- Eliminazione dei dati: quando si rimuove un account amministratore delegato per Audit Manager, i dati di quell'account non vengono eliminati. Se desideri eliminare i dati relativi alle risorse per un account amministratore delegato, è necessario eseguire tale attività separatamente prima di rimuovere l'account. Questa operazione può essere eseguita nella console Gestione audit. In alternativa, puoi utilizzare una delle operazioni API di eliminazione fornite da Gestione audit. Per un elenco delle operazioni di eliminazione disponibili, vedere Eliminazione dei dati di Gestione audit.

  Al momento, Gestione audit non offre un'opzione per eliminare le prove per uno specifico amministratore delegato. Invece, quando il tuo account di gestione annulla la registrazione di

Gestione audit, eseguiamo una pulizia dell'account amministratore delegato corrente al momento dell'annullamento della registrazione.

Prima di aggiungere il nuovo account

Prima di aggiungere il nuovo account amministratore delegato, tieni presenti le seguenti considerazioni:

- Il nuovo account deve far parte di un'organizzazione.
- Prima di designare un nuovo amministratore delegato, è necessario abilitare tutte le funzionalità dell'organizzazione. È inoltre necessario configurare le impostazioni del Security Hub dell'organizzazione. In tal modo, Gestione audit può raccogliere le prove del Security Hub dagli account dei tuoi membri.
- L'account amministratore delegato deve avere accesso alla chiave KMS fornita durante la configurazione di Gestione audit.
- Non puoi utilizzare il tuo account di AWS Organizations gestione come amministratore delegato in Audit Manager.

Procedura

È possibile modificare un amministratore delegato utilizzando la console Gestione audit, AWS Command Line Interface (AWS CLI) o l'API Gestione audit.

> **Warning**
>
> Quando modifichi un amministratore delegato, continui ad avere accesso alle prove raccolte in precedenza con il vecchio account amministratore delegato. Tuttavia, Gestione audit smette di raccogliere e allegare prove al vecchio account amministratore delegato.

Audit Manager console

Per modificare l'attuale amministratore delegato sulla console Audit Manager

1. (Facoltativo) Se l'attuale amministratore delegato (account A) ha abilitato evidence finder, esegui la seguente attività di pulizia:

- Prima di assegnare l'account B come nuovo amministratore delegato, assicurati che l'account A acceda a Gestione audit e disattivi lo strumento evidence finder.

  Disabilitare evidence finder elimina automaticamente l'archivio di dati degli eventi creato quando l'account A ha abilitato evidence finder. Se non completi questo passaggio, l'account A deve accedere a CloudTrail Lake ed eliminare manualmente l'archivio dati degli eventi. In caso contrario, l'Event Data Store rimane nell'account A e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

2. Dalla scheda impostazioni Generali, vai alla sezione Amministratore delegato e scegli Rimuovi.
3. Nella finestra pop-up che appare, scegli Rimuovi per confermare.
4. In ID account amministratore delegato, inserisci l'ID dell'account dell'amministratore delegato.
5. Scegli Delega.

AWS CLI

Per modificare l'attuale amministratore delegato in AWS CLI

Innanzitutto, esegui il deregister-organization-admin-accountcomando utilizzando il `--admin-account-id` parametro per specificare l'ID account dell'amministratore delegato corrente.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Quindi, esegui il register-organization-admin-accountcomando utilizzando il `--admin-account-id` parametro per specificare l'ID account del nuovo amministratore delegato.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Per modificare l'attuale amministratore delegato utilizzando l'API

Innanzitutto, richiama l'DeregisterOrganizationAdminAccountoperazione e utilizza il adminAccountIdparametro per specificare l'ID dell'account dell'attuale amministratore delegato.

Quindi, richiamate l'RegisterOrganizationAdminAccountoperazione e utilizzate il adminAccountIdparametro per specificare l'ID account del nuovo amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Per rimuovere il tuo account amministratore delegato, consulta. Rimozione di un amministratore delegato

Risorse aggiuntive

- Creazione e gestione di un'organizzazione
- Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations

Rimozione di un amministratore delegato

La rimozione dell'account amministratore delegato interrompe l'ulteriore raccolta di prove per quell'account, ma si conserva l'accesso alle prove raccolte in precedenza.

Se è necessario rimuovere l'account di amministratore delegato per Audit Manager, è possibile seguire i passaggi necessari in questa pagina. Segui attentamente i prerequisiti e le procedure, poiché comportano la pulizia delle risorse per evitare costi di archiviazione non necessari.

Prerequisiti

Prima di rimuovere l'account amministratore delegato da Audit Manager, tieni presenti le seguenti considerazioni:

Attività di pulizia di Evidence finder

Se l'attuale amministratore delegato ha abilitato Evidence Finder, è necessario eseguire un'attività di pulizia.

Prima di utilizzare l'account di gestione per rimuovere l'attuale amministratore delegato, assicurati che l'account amministratore delegato corrente acceda a Audit Manager e disattivi lo strumento di ricerca delle prove. Disabilitare evidence finder comporta l'eliminazione automatica di un l'archivio di dati degli eventi creato nell'account quando evidence finder era abilitato.

Se questa attività non viene completata, l'l'archivio di dati degli eventi rimane nel loro account. In questo caso, consigliamo che l'amministratore delegato originale utilizzi CloudTrail Lake per eliminare manualmente l'archivio dati degli eventi.

Questa attività di pulizia è necessaria per assicurarti che non ti ritroverai con più archivi di dati degli eventi. Dopo la rimozione o la modifica di un account amministratore delegato, Gestione audit ignora un archivio di dati degli eventi non utilizzato. Tuttavia, se non elimini l'Event Data Store inutilizzato, l'Event Data Store continua a sostenere costi di archiviazione da parte di Lake. CloudTrail

Eliminazione dei dati

Quando rimuovi un account amministratore delegato per Gestione audit, i dati di quell'account non vengono eliminati. Se desideri eliminare i dati relativi alle risorse per un account amministratore delegato, è necessario eseguire tale attività separatamente prima di rimuovere l'account. Questa operazione può essere eseguita nella console Gestione audit. In alternativa, puoi utilizzare una delle operazioni API di eliminazione fornite da Gestione audit. Per un elenco delle operazioni di eliminazione disponibili, vedere Eliminazione dei dati di Gestione audit.

Al momento, Gestione audit non offre un'opzione per eliminare le prove per uno specifico amministratore delegato. Invece, quando il tuo account di gestione annulla la registrazione di Gestione audit, eseguiamo una pulizia dell'account amministratore delegato corrente al momento dell'annullamento della registrazione.

Procedura

È possibile rimuovere un amministratore delegato utilizzando la console Gestione audit, AWS Command Line Interface (AWS CLI) o l'API Gestione audit.

> **Warning**
>
> Quando rimuovi un amministratore delegato, continui ad avere accesso alle prove raccolte in precedenza con l'account amministratore delegato. Tuttavia, Gestione audit smette di raccogliere e allegare prove al vecchio account amministratore delegato.

Audit Manager console

Per rimuovere l'attuale amministratore delegato dalla console Audit Manager

1. (Facoltativo) Se l'attuale amministratore delegato ha abilitato evidence Finder, esegui la seguente attività di pulizia:

   - Assicurati che l'attuale account amministratore delegato acceda a Gestione audit e disabiliti evidence finder.

     Disabilitare evidence finder elimina automaticamente l'archivio di dati degli eventi creato nel loro account quando hanno abilitato evidence finder. Se questo passaggio non viene completato, l'account amministratore delegato deve utilizzare CloudTrail Lake per eliminare manualmente l'Event Data Store. In caso contrario, l'Event Data Store rimane nel loro account e continua a incorrere nei costi di archiviazione di CloudTrail Lake.
2. Dalla scheda impostazioni Generali, vai alla sezione Amministratore delegato e scegli Rimuovi.
3. Nella finestra pop-up che appare, scegli Rimuovi per confermare.

AWS CLI

Disabilitare evidence finder elimina automaticamente l'archivio di dati degli eventi creato nel loro account quando hanno abilitato evidence finder. Se questo passaggio non viene completato, l'account amministratore delegato deve utilizzare CloudTrail Lake per eliminare manualmente l'Event Data Store. In caso contrario, l'Event Data Store rimane nel loro account e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

Per rimuovere l'attuale amministratore delegato in AWS CLI

Eseguire il deregister-organization-admin-accountcomando e utilizzare il `--admin-account-id` parametro per specificare l'ID dell'account dell'amministratore delegato.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Per rimuovere l'attuale amministratore delegato utilizzando l'API

Chiama l'DeregisterOrganizationAdminAccountoperazione e utilizza il adminAccountIdparametro per specificare l'ID account dell'amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Risorse aggiuntive

- Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations

Configurazione dei proprietari di audit predefiniti

È possibile utilizzare questa impostazione per specificare gli utenti predefiniti audit owner che hanno accesso principale alle valutazioni in Audit Manager.

Procedura

È possibile aggiornare questa impostazione utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Audit Manager console

Puoi scegliere tra Account AWS quelle elencate nella tabella o utilizzare la barra di ricerca per cercarne altre Account AWS.

Per aggiornare i proprietari degli audit predefiniti sulla console Audit Manager

1. Dalla scheda Impostazioni di valutazione, vai alla sezione Proprietari di audit predefiniti e scegli Modifica.
2. Per aggiungere un proprietario di audit predefinito, seleziona la casella di controllo accanto al nome account in Proprietario dell'audit.
3. Per rimuovere un proprietario di audit predefinito, deseleziona la casella di controllo accanto al nome account in Proprietario dell'audit.
4. Al termine, scegli Salva.

AWS CLI

Per aggiornare il proprietario dell'audit predefinito nel AWS CLI

Esegui il comando update-settings e utilizza il parametro `--default-process-owners` per specificare il proprietario dell'audit.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni. Nota che `roleType` può essere solo `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Per aggiornare il proprietario dell'audit predefinito utilizzando l'API

Chiama l'UpdateSettingsoperazione e utilizza il defaultProcessOwnersparametro per specificare i proprietari di audit predefiniti. Nota che `roleType` può essere solo `PROCESS_OWNER`.

Risorse aggiuntive

- Per ulteriori informazioni sui proprietari degli audit, vedere Proprietari degli audit nella sezione Concetti e terminologia di questa guida.

Configurazione della destinazione predefinita del rapporto di valutazione

Quando generi un report di valutazione, Gestione audit pubblica il report nel bucket S3 di tua scelta. Questo bucket S3 è denominato. assessment report destination Puoi scegliere il bucket S3 in cui Audit Manager archivia i tuoi report di valutazione.

Prerequisiti

Suggerimenti di configurazione per la destinazione del rapporto di valutazione

Per garantire la corretta generazione del rapporto di valutazione, ti consigliamo di utilizzare le seguenti configurazioni per la destinazione del rapporto di valutazione.

Bucket della stessa regione

Si consiglia di utilizzare un bucket S3 che rientri nella stessa Regione AWS della valutazione. Se utilizzi un bucket e una valutazione relativi alla stessa area geografica, il rapporto di valutazione può includere fino a 22.000 elementi di prova. Al contrario, quando si utilizza un gruppo e una valutazione in più regioni, è possibile includere solo 3.500 elementi di prova.

Regione AWS

La Regione AWS chiave gestita dal cliente (se ne hai fornita una) deve corrispondere alla regione della valutazione e al bucket S3 di destinazione del rapporto di valutazione. Per istruzioni su come modificare la chiave KMS, consulta. Configurazione delle impostazioni di crittografia dei dati Per un elenco delle Regioni Gestione audit supportate, consulta la sezione Endpoint e quote AWS Audit Managernei Riferimenti generali di Amazon Web Services.

Crittografia del bucket S3

Se la destinazione del rapporto di valutazione ha una policy del bucket che richiede la crittografia lato server (SSE) utilizzando SSE-KMS, la chiave KMS utilizzata in quella policy del bucket deve corrispondere alla chiave KMS configurata nelle impostazioni di crittografia dei dati di Gestione audit. Se non hai configurato una chiave KMS nelle impostazioni di Gestione audit e la policy del bucket di destinazione del rapporto di valutazione richiede SSE, assicurati che la policy del bucket consenta SSE-S3. Per istruzioni su come configurare la chiave KMS utilizzata per la crittografia dei dati, consulta. Configurazione delle impostazioni di crittografia dei dati

Bucket S3 multi-account

L'utilizzo di un bucket S3 per più account come destinazione del rapporto di valutazione non è supportato nella console Gestione audit. È possibile specificare un bucket tra più account come destinazione del rapporto di valutazione utilizzando lo AWS CLI o uno degli AWS SDK, ma per semplicità, ti consigliamo di non farlo. Se scegli di utilizzare un bucket S3 con più account come destinazione del rapporto di valutazione, considera i seguenti punti.

- Per impostazione predefinita, gli oggetti S3, come i report di valutazione, sono di proprietà di chi carica l'oggetto. Account AWS È possibile utilizzare l'impostazione Proprietà dell'oggetto S3 per modificare questo comportamento predefinito affinché tutti i nuovi oggetti scritti da account con la lista di controllo degli accessi (ACL) predefinita `bucket-owner-full-control` diventino automaticamente di proprietà del proprietario del bucket.

  Sebbene non sia un requisito, ti consigliamo di apportare le seguenti modifiche alle impostazioni del bucket tra account. Apportando queste modifiche, il proprietario del bucket ha il pieno controllo dei report di valutazione che pubblichi nel suo bucket.

  - Imposta la proprietà dell'oggetto del bucket S3 sul bucket preferito dal proprietario, anziché sull'autore dell'oggetto predefinito
  - Aggiungi una policy del bucket per garantire che gli oggetti caricati in quel bucket abbiano l'ACL `bucket-owner-full-control`

- Per consentire a Gestione audit di pubblicare report in un bucket S3 tra più account, è necessario aggiungere la seguente policy del bucket S3 alla destinazione del rapporto di valutazione. Sostituisci il *`testo segnaposto`* con le tue informazioni. L'elemento `Principal` di questa policy è l'utente o il ruolo che possiede la valutazione e crea il rapporto di valutazione. Il `Resource` specifica il bucket S3 tra più account in cui viene pubblicato il rapporto.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Procedura

È possibile aggiornare questa impostazione utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Audit Manager console

Per aggiornare la destinazione predefinita del rapporto di valutazione sulla console Audit Manager

1. Dalla scheda Impostazioni di valutazione, vai alla sezione Destinazione del rapporto di valutazione.
2. Per utilizzare un bucket S3 esistente, seleziona il nome del bucket dal menu a discesa.
3. Per creare un nuovo bucket S3, scegli Crea nuovo bucket.
4. Al termine, scegli Salva.

AWS CLI

Per aggiornare la destinazione predefinita del rapporto di valutazione nel AWS CLI

Esegui il comando update-settings e usa il parametro `--default-assessment-reports-destination` per specificare un bucket S3.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://DOC-EXAMPLE-DESTINATION-BUCKET
```

Audit Manager API

Per aggiornare la destinazione predefinita del rapporto di valutazione utilizzando l'API

Chiama l'UpdateSettingsoperazione e utilizza il parametro defaultAssessmentReportsDestination per specificare un bucket S3.

Risorse aggiuntive

- Creazione di un bucket
- Report di valutazione

Configurazione delle notifiche di Audit Manager

Puoi configurare Audit Manager per inviare notifiche all'argomento Amazon SNS di tua scelta. Se sei abbonato a quell'argomento SNS, ricevi notifiche direttamente ogni volta che accedi a Audit Manager.

Segui i passaggi in questa pagina per scoprire come visualizzare e aggiornare le impostazioni di notifica in base alle tue preferenze. Puoi utilizzare un argomento SNS standard o un argomento SNS FIFO (first-in-first-out). Sebbene Gestione audit supporti l'invio di notifiche agli argomenti FIFO, l'ordine in cui vengono inviati i messaggi non è garantito.

Prerequisiti

Se desideri utilizzare un argomento Amazon SNS di cui non sei proprietario, devi configurare la tua policy AWS Identity and Access Management (IAM) per questo. In particolare, devi configurarla per consentire la pubblicazione dal nome della risorsa Amazon (ARN) dell'argomento. Per un esempio di policy che puoi usare, consultaEsempio 1 (Autorizzazioni per l'argomento SNS).

Procedura

È possibile aggiornare questa impostazione utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Audit Manager console

Per aggiornare le impostazioni di notifica sulla console Audit Manager

1. Dalla scheda Impostazioni di valutazione, vai alla sezione Notifiche.
2. Per utilizzare un argomento SNS esistente, seleziona il nome dell'argomento nel menu a discesa.
3. Per creare un nuovo argomento SNS, scegli Crea nuovo argomento.
4. Al termine, scegli Salva.

AWS CLI

Per aggiornare le impostazioni di notifica in AWS CLI

Esegui il comando aggiorna le impostazioni e usa il parametro `--sns-topic` per specificare un argomento SNS.

Nell'esempio seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Per aggiornare le impostazioni di notifica utilizzando l'API

Chiama l'UpdateSettingsoperazione e utilizza il parametro SNSTOpic per specificare un argomento SNS.

Risorse aggiuntive

- Per informazioni sulla creazione di un argomento Amazon SNS, consulta Creazione di un argomento Amazon SNS nella Guida per l'utente di Amazon SNS.
- Per un esempio di policy che puoi utilizzare per consentire all'Audit Manager di inviare notifiche su argomenti di Amazon SNS, consulta Esempio 1 (Autorizzazioni per l'argomento SNS)
- Per ulteriori informazioni sull'elenco delle azioni che richiamano le notifiche in Gestione audit, consulta Notifiche in AWS Audit Manager.
- Per le soluzioni ai problemi di notifica in Audit Manager, vedereRisoluzione dei problemi di notifica .

Attivazione di evidence finder

Puoi abilitare la funzione di ricerca delle prove in Audit Manager per cercare prove nel tuo Account AWS. Se sei un amministratore delegato di Audit Manager, puoi cercare prove per tutti gli account dei membri della tua organizzazione.

Segui questi passaggi per scoprire come abilitare lo strumento di ricerca delle prove. Presta molta attenzione ai prerequisiti, poiché avrai bisogno di autorizzazioni specifiche per creare e gestire un archivio dati di eventi in CloudTrail Lake per questa funzionalità.

Prerequisiti

Autorizzazioni necessarie per abilitare evidence finder

Per abilitare Evidence Finder, hai bisogno delle autorizzazioni per creare e gestire un archivio di dati di eventi in Lake. CloudTrail Per utilizzare la funzione, sono necessarie le autorizzazioni per eseguire CloudTrail le query su Lake. Per un esempio di politica di autorizzazione che puoi utilizzare, vedi. Esempio 4 (Autorizzazioni per abilitare Evidence Finder)

Se hai bisogno di assistenza con le autorizzazioni, contatta AWS l'amministratore. Se sei un amministratore AWS , puoi copiare la dichiarazione di autorizzazione richiesta e allegarla a una policy IAM.

Procedura

Richiesta di attivazione di evidence finder

È possibile completare questa attività utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

> **Note**
>
> È necessario abilitare lo strumento di ricerca delle prove in ogni Regione AWS area in cui si desidera cercare prove.

Audit Manager console

Per richiedere l'attivazione di Evidence Finder sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Dalla scheda delle impostazioni di Evidence finder, vai alla sezione Evidence finder.
3. Scegli la politica di autorizzazione richiesta, quindi le autorizzazioni di View CloudTrail Lake per visualizzare le autorizzazioni richieste per Evidence Finder. Se non disponi già di queste autorizzazioni, puoi copiare questa dichiarazione di policy e allegarla a una policy IAM.
4. Scegli Abilita .
5. Nella finestra a comparsa, scegli Richiedi di abilitare.

AWS CLI

Per richiedere di abilitare Evidence Finder nel AWS CLI

Esegui il comando update-settings con il parametro `--evidence-finder-enabled`.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Per richiedere di abilitare Evidence Finder utilizzando l'API

Chiama l'UpdateSettingsoperazione e usa il evidenceFinderEnabledparametro.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Dopo aver richiesto di abilitare Evidence Finder, puoi controllare lo stato della tua richiesta. Per istruzioni, consulta Conferma dello stato di Evidence Finder .

Risorse aggiuntive

- Evidence finder
- Risoluzione dei problemi in Evidence Finder

Conferma dello stato di Evidence Finder

Dopo aver inviato la richiesta per abilitare Evidence Finder, sono necessari fino a 10 minuti per abilitare la funzionalità e creare un archivio dati sugli eventi. Dal momento in cui viene creato l'archivio di dati degli eventi, tutte le nuove prove vengono inserite nell'archivio di dati degli eventi.

Quando evidence finder è abilitato e viene creato l'archivio di dati degli eventi, riempiamo il nuovo archivio di dati degli eventi con un massimo di due anni di prove passate. Questo processo avviene automaticamente e richiede fino a sette giorni per essere completato.

Segui i passaggi in questa pagina per verificare e comprendere lo stato della tua richiesta di abilitare Evidence Finder.

Prerequisiti

Assicurati di aver seguito i passaggi per abilitare Evidence Finder. Per istruzioni, consulta Attivazione di evidence finder.

Procedura

È possibile verificare lo stato attuale di evidence finder utilizzando la console Gestione audit, AWS CLI, o l'API Gestione audit.

Audit Manager console

Per visualizzare lo stato attuale di Evidence Finder sulla console Audit Manager

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. In Abilita evidence finder - facoltativo, rivedi lo stato corrente.

   Ogni stato è definito nel modo seguente:

Stato	Descrizione
Il cercatore di prove non è abilitato	Non hai ancora abilitato con successo il cercatore di prove.
Hai richiesto di abilitare lo strumento di ricerca delle prove	La tua richiesta è in attesa della creazione del data store degli eventi.
Il cercatore di prove è abilitato	L'archivio dati degli eventi è stato creato. È ora possibile utilizzare evidence finder. A seconda della quantità di prove a tua disposizione, occorrono fino a sette giorni per riempire il nuovo archivio di dati degli eventi i dati relativi alle prove precedenti. Un

Stato	Descrizione
	pannello informativo blu indica che il riempimento dei dati è in corso. Nel frattempo, sentiti libero di iniziare a esplorare evidence finder. Tuttavia, tieni presente che non tutti i dati sono disponibili fino al completamento del riempimento.
Hai richiesto di disabilit are Evidence Finder	La tua richiesta è in attesa che l'Event Data Store venga eliminato.
Il cercatore di prove è stato disabilitato	Evidence Finder è stato disabilitato in modo permanente e l'archivio dati degli eventi è stato eliminato.

AWS CLI

Per visualizzare lo stato attuale di Evidence Finder nel AWS CLI

Esegui il comando get-settings con il parametro `--attribute` impostato su `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Questa procedura restituisce le seguenti informazioni:

enablementStatus

Questo attributo mostra lo stato attuale di evidence finder.

- `ENABLE_IN_PROGRESS`: hai richiesto di abilitare evidence finder. È attualmente in fase di creazione un archivio di dati degli eventi per supportare le query di evidence finder.
- `ENABLED`: è stato creato un archivio di dati degli eventi ed evidence finder è abilitato. Ti consigliamo di attendere sette giorni prima che l'archivio di dati degli eventi venga riempito con i dati relativi alle prove precedenti. Nel frattempo puoi utilizzare evidence finder, ma non tutti i dati sono disponibili fino al completamento del riempimento.
- `DISABLE_IN_PROGRESS`: hai richiesto di disabilitare evidence finder e la tua richiesta è in attesa che l'archivio di dati degli eventi venga eliminato.
- `DISABLED`: hai disabilitato permanentemente evidence finder e l'archivio di dati degli eventi risulta eliminato. Dopo questa azione non puoi riattivare evidence finder.

backfillStatus

Questo attributo mostra lo stato attuale del riempimento dei dati delle prove.

- `NOT_STARTED`: il riempimento non è ancora iniziato.
- `IN_PROGRESS`: il riempimento è in corso. Il completamento di questa operazione richiede fino a sette giorni, a seconda della quantità di dati di prova.
- `COMPLETED`: il riempimento è stato completato. Tutte le tue prove passate sono ora interrogabili.

Audit Manager API

Per visualizzare lo stato attuale di Evidence Finder utilizzando l'API

Chiama l'GetSettingsoperazione con il `attribute` parametro impostato su. `EVIDENCE_FINDER_ENABLEMENT` Questa procedura restituisce le seguenti informazioni:

enablementStatus

Questo attributo mostra lo stato attuale di evidence finder.

- `ENABLE_IN_PROGRESS`: hai richiesto di abilitare evidence finder. È attualmente in fase di creazione un archivio di dati degli eventi per supportare le query di evidence finder.
- `ENABLED`: è stato creato un archivio di dati degli eventi ed evidence finder è abilitato. Ti consigliamo di attendere sette giorni prima che l'archivio di dati degli eventi venga riempito con i dati relativi alle prove precedenti. Nel frattempo puoi utilizzare evidence finder, ma non tutti i dati sono disponibili fino al completamento del riempimento.
- `DISABLE_IN_PROGRESS`: hai richiesto di disabilitare evidence finder e la tua richiesta è in attesa della cancellazione dell'archivio di dati degli eventi.
- `DISABLED`: hai disabilitato permanentemente evidence finder e l'archivio di dati degli eventi risulta eliminato. Dopo questa azione non puoi riattivare evidence finder.

backfillStatus

Questo attributo mostra lo stato attuale del riempimento dei dati delle prove.

- `NOT_STARTED` significa che il riempimento non è ancora iniziato.

- `IN_PROGRESS` significa che il riempimento è in corso. Il completamento di questa operazione richiede fino a sette giorni, a seconda della quantità di dati di prova.
- `COMPLETED` significa che il riempimento è completo. Tutte le tue prove passate sono ora interrogabili.

Per ulteriori informazioni, consulta la evidenceFinderEnablementGuida di riferimento all'API Audit Manager.

Passaggi successivi

Dopo aver abilitato correttamente Evidence Finder, puoi iniziare a utilizzare la funzione. Ti consigliamo di attendere sette giorni prima che l'archivio di dati degli eventi venga riempito con i dati relativi alle prove precedenti. Nel frattempo puoi utilizzare Evidence Finder, ma è possibile che non tutti i dati siano disponibili fino al completamento del backfill.

Per iniziare a usare Evidence Finder, vedi. Ricerca di prove in Evidence Finder

Risorse aggiuntive

- Risoluzione dei problemi in Evidence Finder

Disabilitare evidence finder

Se non desideri più utilizzare Evidence Finder, puoi disabilitare la funzione in qualsiasi momento.

Segui questi passaggi per scoprire come disabilitare Evidence Finder. Presta molta attenzione ai prerequisiti, poiché avrai bisogno di autorizzazioni specifiche per eliminare l'archivio di dati sugli eventi in CloudTrail Lake che è stato creato quando hai abilitato Evidence Finder.

Prerequisiti

Autorizzazioni necessarie per disabilitare evidence finder

Per disabilitare Evidence Finder, hai bisogno delle autorizzazioni per eliminare un archivio di dati di eventi in Lake. CloudTrail Per un esempio di policy che puoi utilizzare, consulta Autorizzazioni per disabilitare evidence finder.

Se hai bisogno di assistenza con le autorizzazioni, contatta il tuo amministratore. AWS Se sei un amministratore AWS , puoi allegare la dichiarazione di autorizzazione richiesta per una policy IAM.

Procedura

È possibile completare questa attività utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

> **Warning**
>
> La disabilitazione di Evidence Finder elimina il CloudTrail Lake Event Data Store creato da Audit Manager. Di conseguenza, non puoi riattivare la funzionalità. Per riutilizzare evidence finder dopo averlo disabilitato, devi disabilitare AWS Audit Managere quindi riattivare completamente il servizio.

Audit Manager console

Per disabilitare lo strumento di ricerca delle prove sulla console Audit Manager

1. Nella sezione Evidence finder della pagina delle impostazioni di Gestione audit, scegli Disabilita.
2. Nella finestra a comparsa che appare, inserisci **`Yes`** per confermare la decisione.
3. Scegli Richiedi di disabilitare.

AWS CLI

Per disabilitare lo strumento di ricerca delle prove in AWS CLI

Esegui il comando update-settings con il parametro `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Per disabilitare Evidence Finder utilizzando l'API

Chiama l'UpdateSettingsoperazione e usa il evidenceFinderEnabledparametro.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK specifici della lingua AWS .

Risorse aggiuntive

- Risoluzione dei problemi in Evidence Finder

Configurazione della destinazione di esportazione predefinita per Evidence Finder

Quando esegui query in Evidence Finder, puoi esportare i risultati della ricerca in un file con valori separati da virgole (CSV). Utilizza questa impostazione per scegliere il bucket S3 predefinito in cui Gestione audit salva i file esportati.

Prerequisiti

Il bucket S3 deve disporre della politica di autorizzazioni richiesta per consentire la scrittura dei file di esportazione al suo interno. CloudTrail Più specificamente, la policy del bucket deve includere un'`s3:PutObject`azione e l'ARN del bucket ed essere elencata CloudTrail come principale del servizio.

- Per un esempio di politica di autorizzazione che puoi utilizzare, vedi. Esempio 3 (autorizzazioni di esportazione di destinazione)
- Per istruzioni su come allegare questa policy al tuo bucket S3, consulta Aggiungere una policy bucket utilizzando la console Amazon S3.
- Per ulteriori suggerimenti, vedi i suggerimenti di configurazione per la destinazione di esportazione in questa pagina.

Suggerimenti di configurazione per la destinazione di esportazione

Per garantire una corretta esportazione del file, ti consigliamo di verificare le seguenti configurazioni per la destinazione di esportazione.

Regione AWS

La Regione AWS chiave gestita dal cliente (se ne hai fornita una) deve corrispondere alla regione della valutazione. Per istruzioni su come modificare la chiave KMS, consulta Impostazioni di crittografia dei dati Gestione audit.

Bucket S3 multi-account

L'utilizzo di un bucket S3 per più account come destinazione dell'esportazione non è supportato nella console Gestione audit. È possibile specificare un bucket tra più account utilizzando uno AWS CLI o uno degli AWS SDK, ma per semplicità, ti consigliamo di non farlo. Se scegli di utilizzare un bucket S3 con più account come destinazione dell'esportazione, considera i seguenti punti.

- Per impostazione predefinita, gli oggetti S3, come le esportazioni in formato CSV, sono di proprietà di chi carica l'oggetto. Account AWS È possibile utilizzare l'impostazione Proprietà dell'oggetto S3 per modificare questo comportamento predefinito affinché tutti i nuovi oggetti scritti da account con la lista di controllo degli accessi (ACL) predefinita `bucket-owner-full-control` diventino automaticamente di proprietà del proprietario del bucket.

  Sebbene non sia un requisito, ti consigliamo di apportare le seguenti modifiche alle impostazioni del bucket tra account. Apportando queste modifiche, il proprietario del bucket ha il pieno controllo dei file esportati che pubblichi nel suo bucket.

  - Imposta la proprietà dell'oggetto del bucket S3 sul bucket preferito dal proprietario, anziché sull'autore dell'oggetto predefinito
  - Aggiungi una policy del bucket per garantire che gli oggetti caricati in quel bucket abbiano l'ACL `bucket-owner-full-control`
- Per consentire a Gestione audit di esportare i file in un bucket S3 con più account, è necessario aggiungere la seguente policy del bucket S3 al bucket di destinazione dell'esportazione. Sostituisci il *`testo segnaposto`* con le tue informazioni. L'elemento `Principal` di questa policy è l'utente o il ruolo attribuito alla valutazione ed esportazione del file. `Resource` specifica il bucket S3 multi-account in cui viene esportato il file.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
```

```
                "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Procedura

È possibile aggiornare questa impostazione utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Audit Manager console

Per aggiornare le impostazioni della destinazione di esportazione sulla console Audit Manager

1. Dalla scheda delle impostazioni di Evidence finder, vai alla sezione Destinazione di esportazione.
2. Selezionare una delle seguenti opzioni:
   - Se desideri rimuovere il bucket S3 corrente, scegli Rimuovi per cancellare le impostazioni.
   - Se desideri salvare un bucket S3 predefinito per la prima volta, procedi alla fase 3.
3. Specifica il bucket S3 in cui desideri archiviare i file esportati.
   - Scegli Sfoglia S3 per scegliere da un elenco dei tuoi bucket.
   - In alternativa, puoi inserire l'URI del bucket in questo formato: **`s3://bucketname/prefix`**

> **Tip**
>
> Per mantenere organizzato il bucket di destinazione, puoi creare una cartella opzionale per le esportazioni in formato CSV. A tale scopo, aggiungi una barra (**/**) e un prefisso al valore nella casella URI di risorsa (ad esempio, **/evidenceFinderCSVExports**). Gestione audit include quindi questo prefisso quando aggiunge il file CSV al bucket e Amazon S3 genera il percorso specificato dal prefisso. Per ulteriori informazioni sui prefissi in Amazon S3, vedi Organizzare oggetti nella console Amazon S3 nella Guida per l'utente Amazon Simple Storage Service.

4. Al termine, scegli Salva.

Per istruzioni su come creare un bucket S3, vedi Crea un bucket nella Guida Utente Amazon S3.

AWS CLI

Per aggiornare le impostazioni della destinazione di esportazione nel AWS CLI

Esegui il comando update-settings e usa il parametro `--default-export-destination` per specificare un bucket S3.

Nell'esempio seguente, sostituisci ciascun *`testo segnaposto`* con le tue informazioni:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=DOC-EXAMPLE-DESTINATION-BUCKET
```

Per istruzioni su come creare un bucket S3, vedi crea-bucket nella Riferimento ai comandi AWS CLI .

Audit Manager API

Per aggiornare le impostazioni della destinazione di esportazione utilizzando l'API

Chiama l'UpdateSettingsoperazione e usa il defaultExportDestinationparametro per specificare un bucket S3.

Per istruzioni su come creare un bucket S3, consulta CreateBucketAmazon S3 API Reference.

Notifiche in AWS Audit Manager

AWS Audit Manager può informarti sulle azioni degli utenti tramite Amazon Simple Notification Service (Amazon SNS).

Gestione audit invia notifiche quando si verifica uno dei seguenti eventi:

- Il titolare dell'audit delega un set di controllo per la revisione.
- Un delegato invia un set di controllo revisionato al proprietario dell'audit.
- Il proprietario dell'audit completa la revisione di un set di controlli.

Risorse aggiuntive

- Per configurare le notifiche in Audit Manager, consultaConfigurazione delle notifiche di Audit Manager.
- Per trovare le risposte a domande e problemi comuni, Risoluzione dei problemi di notifica consulta la sezione Risoluzione dei problemi di questa guida.

Risoluzione dei problemi più comuni in AWS Audit Manager

Durante l'utilizzo AWS Audit Manager, potresti riscontrare determinati problemi o sfide che richiedono la risoluzione dei problemi. Che tu stia affrontando difficoltà nell'impostazione delle valutazioni, nella raccolta di prove o in qualsiasi altro aspetto del servizio, puoi utilizzare questa guida alla risoluzione dei problemi per trovare i nostri consigli che ti aiutano a risolvere i problemi più comuni in modo rapido ed efficiente.

Ti invitiamo a consultare l'elenco di argomenti riportato di seguito, a trovare quello più adatto al tuo scenario e a seguire le indicazioni fornite per tornare in pista. Seguendo i passaggi di risoluzione dei problemi forniti, è possibile risolvere il problema in modo indipendente e continuare a sfruttare tutte le funzionalità di Audit Manager. Tuttavia, se il problema specifico non è trattato qui o non riesci a risolverlo dopo aver seguito i passaggi consigliati, ti consigliamo di contattare AWS Supportper ulteriore assistenza.

Argomenti

Risoluzione dei problemi di valutazione e raccolta di prove

È possibile utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti la valutazione e la raccolta di prove in Gestione audit.

Problemi relativi alla raccolta delle prove

- La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub
- La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Config
- La mia valutazione non sta raccogliendo prove dell'attività degli utenti da AWS CloudTrail
- La mia valutazione non sta raccogliendo prove dei dati di configurazione per una chiamata AWS API
- Un controllo comune non consiste nella raccolta di prove automatizzate
- Le mie prove vengono generate a intervalli diversi e non sono sicuro della frequenza con cui vengono raccolte
- Ho disabilitato e poi riabilitato Gestione audit e ora le mie valutazioni preesistenti non raccolgono più prove
- Nella pagina dei dettagli della mia valutazione, mi viene richiesto di ricreare la mia valutazione
- Qual è la differenza tra una fonte di dati e una fonte di prove?

Problemi di valutazione

- La creazione della mia valutazione non è riuscita
- Cosa succede se rimuovo un account in ambito dalla mia organizzazione?
- Non riesco a visualizzare i servizi oggetto della mia valutazione
- Non riesco a modificare i servizi in ambito per la mia valutazione
- Qual è la differenza tra un servizio in ambito e un tipo di origine dati?

Ho creato una valutazione ma non riesco ancora a visualizzare alcuna prova

Se non riesci a visualizzare alcuna prova, è probabile che tu non abbia aspettato almeno 24 ore dopo aver creato la valutazione o che si sia verificato un errore di configurazione.

Ti consigliamo di controllare quanto segue:

1. Assicurati che siano trascorse 24 ore dalla creazione della valutazione. Le prove automatiche diventano disponibili 24 ore dopo la creazione della valutazione.
2. Assicurati di utilizzare Audit Manager nello Regione AWS stesso modo in Servizio AWS cui ti aspetti di vedere le prove.

3. Se ti aspetti di vedere le prove dei controlli di conformità provenienti da AWS Config e AWS Security Hub, assicurati che sia la console Security Hub che la AWS Config console Security Hub mostrino i risultati di questi controlli. I risultati di AWS Config and Security Hub dovrebbero essere visualizzati nello stesso Regione AWS modo in cui si utilizza Audit Manager.

Se non riesci ancora a vedere prove nella tua valutazione e ciò non è dovuto a uno dei problemi indicati, controlla le altre potenziali cause descritte in questa pagina.

La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub

Se non vedi le prove della verifica di conformità relative a un AWS Security Hub controllo, ciò potrebbe essere dovuto a uno dei seguenti problemi.

Configurazione mancante in AWS Security Hub

Questo problema può presentarsi se hai saltato alcuni passaggi di configurazione quando hai abilitato AWS Security Hub.

Per risolvere questo problema, assicurati di aver abilitato Security Hub con le impostazioni richieste per Audit Manager. Per istruzioni, consulta Abilita e configura AWS Security Hub (facoltativo).

Un nome di controllo di Security Hub è stato inserito erroneamente nel tuo **`ControlMappingSource`**

Quando utilizzi l'API Gestione audit per creare un controllo personalizzato, puoi specificare un controllo Security Hub come mappatura dell'origine dati per la raccolta delle prove. A tale scopo, devi immette un ID di controllo come `keywordValue`.

Se non vedi le prove del controllo di conformità relative a un controllo di Security Hub, è possibile che `keywordValue` sia stato inserito erroneamente nella tua `ControlMappingSource`. `keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. Se inserita in modo errato, Gestione audit potrebbe non riconoscere quella regola. Di conseguenza, potresti non raccogliere le prove relative al controllo di conformità per tale controllo come previsto.

Per risolvere il problema, aggiorna il controllo personalizzato e modifica il `keywordValue`. Il formato corretto di una parola chiave di Security Hub varia. Per una maggiore precisione, consulta l'elenco diControlli Security Hub supportati .

`AuditManagerSecurityHubFindingsReceiver`Manca EventBridge la regola di Amazon

Quando abiliti Audit Manager, una regola denominata `AuditManagerSecurityHubFindingsReceiver` viene automaticamente creata e abilitata in Amazon EventBridge. Questa regola consente a Gestione audit di raccogliere gli esiti di Security Hub come prova.

Se questa regola non è elencata e abilitata nel Regione AWS luogo in cui utilizzi Security Hub, Audit Manager non può raccogliere i risultati del Security Hub per quella regione.

Per risolvere il problema, accedi alla EventBridge console e conferma che la `AuditManagerSecurityHubFindingsReceiver` regola esista nel tuo Account AWS. Se la regola non esiste, ti consigliamo di disabilitare Gestione audit e quindi riattivare il servizio. Se questa azione non risolve il problema o se la disabilitazione di Gestione audit non è un'opzione, contatta AWS Supportper ricevere assistenza.

AWS Config Regole collegate ai servizi create da Security Hub

Tieni presente che Audit Manager non raccoglie prove dalle AWS Config regole collegate ai servizi create da Security Hub. Si tratta di un tipo specifico di AWS Config regola gestita abilitata e controllata dal servizio Security Hub. Security Hub crea istanze di queste regole collegate ai servizi nell' AWS ambiente, anche se esistono già altre istanze delle stesse regole. Di conseguenza, per evitare la duplicazione delle prove, Gestione audit non supporta la raccolta di prove dalle regole collegate ai servizi.

Ho disabilitato un controllo di sicurezza in Security Hub. Audit Manager raccoglie le prove dei controlli di conformità per quel controllo di sicurezza?

Audit Manager non raccoglie prove relative alla disabilitazione dei controlli di sicurezza.

Se si imposta lo stato di un controllo di sicurezza su disabilitato in Security Hub, non viene eseguito alcun controllo di sicurezza per quel controllo nell'account e nella regione correnti. Di conseguenza, non sono disponibili risultati di sicurezza in Security Hub e nessuna prova correlata viene raccolta da Audit Manager.

Rispettando lo stato di disabilitazione impostato in Security Hub, Audit Manager garantisce che la valutazione rifletta accuratamente i controlli di sicurezza attivi e i risultati pertinenti all'ambiente, esclusi i controlli che hai intenzionalmente disabilitato.

Ho impostato lo stato di un risultato su **`Suppressed`** Security Hub. Audit Manager raccoglie prove di verifica della conformità relative a tale risultato?

Audit Manager raccoglie prove dei controlli di sicurezza che hanno soppresso i risultati.

Se imposti lo stato del flusso di lavoro di un risultato su soppresso in Security Hub, significa che hai esaminato il risultato e non ritieni necessaria alcuna azione. In Audit Manager, questi risultati soppressi vengono raccolti come prove e allegati alla valutazione. I dettagli delle prove mostrano lo stato della valutazione `SUPPRESSED` segnalato direttamente da Security Hub.

Questo approccio garantisce che la valutazione dell'Audit Manager rappresenti accuratamente i risultati di Security Hub, fornendo al contempo visibilità su eventuali risultati soppressi che potrebbero richiedere un'ulteriore revisione o considerazione in un audit.

La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Config

Se non vedi le prove del controllo di conformità relative a una AWS Config regola, ciò potrebbe essere dovuto a uno dei seguenti problemi.

L'identificatore della regola è stato inserito in modo errato nella tua **`ControlMappingSource`**

Quando si utilizza l'API Audit Manager per creare un controllo personalizzato, è possibile specificare una AWS Config regola come mappatura dell'origine dati per la raccolta delle prove. Il `keywordValue` specificato dipende dal tipo di regola.

Se non vedi le prove relative al controllo di conformità relative a una AWS Config regola, è possibile che sia `keywordValue` stata inserita erroneamente nella tua. `ControlMappingSource` `keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. Se inserita in modo errato, Gestione audit potrebbe non riconoscere la regola. Di conseguenza, potresti non raccogliere le prove relative alla controllo di conformità per quella regola come previsto.

Per risolvere il problema, aggiorna il controllo personalizzato e modifica il `keywordValue`.

- Per le regole personalizzate, assicurati che `keywordValue` abbia il prefisso `Custom_` seguito dal nome della regola personalizzata. Il formato del nome della regola personalizzata può variare. Per una maggiore precisione, accedi alla console AWS Configper verificare i nomi delle regole personalizzate.

- Per le regole gestite, assicurati che `keywordValue` sia l'identificatore della regola inserito in `ALL_CAPS_WITH_UNDERSCORES`. Ad esempio, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Per una maggiore precisione, consulta l'elenco delle parole chiave supportate per le regole gestite.

> **Note**
>
> Per alcune regole gestite, l'identificatore della regola è diverso dal nome della regola. Ad esempio, l'identificatore della regola per restricted-ssh è `INCOMING_SSH_DISABLED`. Assicurati di utilizzare l'identificatore della regola, non il nome della regola. Per trovare un identificatore della regola, scegli una regola dall'elenco delle regole gestite e cerca il relativo valore Identificatore.

La regola è una regola collegata al servizio AWS Config

Puoi utilizzare regole gestite e regole personalizzate come mappatura dell'origine dati per la raccolta di prove. Tuttavia, Gestione audit non raccoglie prove dalla maggior parte delle regole collegate ai servizi.

Esistono solo due tipi di regole collegate ai servizi da cui Gestione audit raccoglie prove:

- Regole collegate ai servizi di Conformance Pack
- Regole collegate ai servizi di AWS Organizations

Gestione audit non raccoglie prove da altre regole collegate ai servizi, in particolare da regole con un nome della risorsa Amazon (ARN) che contenga il seguente prefisso: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

Il motivo per cui Gestione audit non raccoglie prove dalla maggior parte delle regole AWS Config collegate ai servizi è quello di evitare prove duplicate nelle valutazioni. Una regola collegata ai servizi è un tipo specifico di regola gestita che consente ad altri di Servizi AWS creare AWS Config regole nell'account dell'utente. Ad esempio, alcuni controlli Security Hub utilizzano una regola AWS Config collegata al servizio per eseguire i controlli di sicurezza. Per ogni controllo Security Hub che utilizza una AWS Config regola collegata al servizio, Security Hub crea un'istanza della AWS Config regola richiesta AWS nell'ambiente. Ciò accade anche se la regola originale esiste già nel tuo account. Pertanto, per evitare di raccogliere due volte le stesse prove dalla stessa regola, Gestione audit ignora la regola collegata ai servizi e non raccoglie prove da essa.

AWS Config non è abilitato

AWS Config deve essere abilitato nel tuo Account AWS. Dopo la configurazione AWS Config in questo modo, Audit Manager raccoglie le prove ogni volta che viene effettuata la valutazione di una AWS Config regola. Assicurati di aver abilitato AWS Config il tuo Account AWS. Per istruzioni, consulta Abilita e configura AWS Config.

La AWS Config regola ha valutato la configurazione di una risorsa prima di impostare la valutazione

Se la AWS Config regola è impostata per valutare le modifiche alla configurazione per una risorsa specifica, è possibile che si verifichi una mancata corrispondenza tra la valutazione AWS Config e le evidenze in Audit Manager. Ciò accade se la valutazione della regola è avvenuta prima che fosse impostato il controllo nella tua valutazione di Gestione audit. In questo caso, Gestione audit non genera prove finché la risorsa sottostante non cambi nuovamente stato e non attivi una rivalutazione della regola.

Come soluzione alternativa, puoi accedere alla regola nella AWS Config console e rivalutarla manualmente. Ciò richiama una nuova valutazione di tutte le risorse relative a quella regola.

La mia valutazione non sta raccogliendo prove dell'attività degli utenti da AWS CloudTrail

Quando si utilizza l'API Audit Manager per creare un controllo personalizzato, è possibile specificare un nome di CloudTrail evento come mappatura dell'origine dati per la raccolta delle prove. A tale scopo, devi inserire il nome dell'evento come `keywordValue`.

Se non vedi le prove dell'attività dell'utente relative a un CloudTrail evento, è possibile che sia `keywordValue` stata inserita erroneamente nel tuo. `ControlMappingSource` `keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. Se lo inserisci in modo errato, Gestione audit potrebbe non riconoscere il nome dell'evento. Di conseguenza, potresti non raccogliere le prove dell'attività dell'utente per quell'evento come previsto.

Per risolvere il problema, aggiorna il controllo personalizzato e modifica il `keywordValue`. Assicurati che l'evento sia scritto come `serviceprefix_ActionName`. Ad esempio, `cloudtrail_StartLogging`. Per una maggiore precisione, Servizio AWS rivedi il prefisso e i nomi delle azioni in Service Authorization Reference.

La mia valutazione non sta raccogliendo prove dei dati di configurazione per una chiamata AWS API

Quando si utilizza l'API Audit Manager per creare un controllo personalizzato, è possibile specificare una chiamata AWS API come mappatura dell'origine dati per la raccolta delle prove. A tale scopo, inserisci la chiamata API come `keywordValue`.

Se non vedi le prove dei dati di configurazione per una chiamata AWS API, è possibile che siano `keywordValue` state inserite in modo errato nel tuo. `ControlMappingSource` `keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. In caso di inserimento errato, Gestione audit potrebbe non riconoscere la chiamata API. Di conseguenza, potresti non raccogliere le prove dei dati di configurazione per quella chiamata API come previsto.

Per risolvere il problema, aggiorna il controllo personalizzato e modifica il `keywordValue`. Assicurati che la chiamata API sia scritta come `serviceprefix_ActionName`. Ad esempio, `iam_ListGroups`. Per una maggiore precisione, consulta l'elenco di. AWS Chiamate API supportate da AWS Audit Manager

Un controllo comune non consiste nella raccolta di prove automatizzate

Quando esamini un controllo comune, potresti visualizzare il seguente messaggio: Questo controllo comune non raccoglie prove automatiche dai controlli principali.

Ciò significa che nessuna fonte di prove AWS gestita può attualmente supportare questo controllo comune. Di conseguenza, la scheda Fonti di evidenza è vuota e non viene visualizzato alcun controllo di base.

Quando un controllo comune non raccoglie prove automatizzate, viene definito controllo comune manuale. I controlli manuali comuni richiedono in genere la fornitura di registrazioni e firme fisiche o dettagli sugli eventi che si verificano al di fuori dell' AWS ambiente. Per questo motivo, spesso non esistono fonti di AWS dati in grado di fornire prove a sostegno dei requisiti del controllo.

Se un controllo comune è manuale, è comunque possibile utilizzarlo come fonte di evidenza per un controllo personalizzato. L'unica differenza è che il controllo comune non raccoglierà automaticamente alcuna prova. Dovrai invece caricare manualmente le tue prove a supporto dei requisiti del controllo comune.

Per aggiungere prove a un controllo comune manuale

1. Crea un controllo personalizzato

- Segui i passaggi per creare o modificare un controllo personalizzato.
- Quando specifichi le fonti di prova nel passaggio 2, scegli il controllo comune manuale come fonte di prova.

2. Crea un framework personalizzato
   - Segui i passaggi per creare o modificare un framework personalizzato.
   - Quando specifichi un set di controlli nel passaggio 2, includi il nuovo controllo personalizzato.
3. Crea una valutazione
   - Segui i passaggi per creare una valutazione dal tuo framework personalizzato.
   - A questo punto, il controllo comune manuale è ora una fonte di evidenza in un controllo di valutazione attivo.
4. Carica prove manuali
   - Segui i passaggi per aggiungere prove manuali al controllo nella tua valutazione.

> **Note**
>
> Man mano che in futuro saranno disponibili più fonti di AWS dati, è possibile che il controllo comune AWS venga aggiornato per includere i controlli di base come fonti di evidenza. In questo caso, se il controllo comune è una fonte di prove in uno o più dei controlli di valutazione attivi, trarrai automaticamente vantaggio da questi aggiornamenti. Non sono necessarie ulteriori configurazioni da parte tua e inizierai a raccogliere prove automatizzate a supporto del controllo comune.

Le mie prove vengono generate a intervalli diversi e non sono sicuro della frequenza con cui vengono raccolte

I controlli nelle valutazioni di Gestione audit sono mappati su varie origini dati. Ogni origine dati ha una frequenza di raccolta delle prove diversa. Di conseguenza, non esiste una one-size-fits-all risposta alla frequenza con cui vengono raccolte le prove. Alcune origini dati valutano la conformità, mentre altre acquisiscono solo lo stato delle risorse e modificano i dati senza una determinazione della conformità.

Di seguito è riportato un riepilogo dei diversi tipi di origini dati e della frequenza con cui raccolgono le prove.

Tipo di origine dati	Descrizione	Frequenza di raccolta delle prove	Quando questo controllo è attivo in una valutazione
AWS CloudTrail	Tiene traccia di un'attività specifica dell'utente.	Continuo	Audit Manager filtra CloudTrail i log in base alla parola chiave scelta. I log elaborati vengono importati come prove dell'attività dell'utente.
AWS Security Hub	Acquisisce uno snapshot della posizione di sicurezza delle risorse segnalando gli esiti da Security Hub.	In base alla pianificazione del controllo di Security Hub (in genere ogni 12 ore circa)	Gestione audit recupera gli esiti di sicurezza direttamente da Security Hub. Il risultato viene importato come prova del controllo di conformità.
AWS Config	Acquisisce un'istantanea del vostro stato di sicurezza delle risorse riportando i risultati di. AWS Config	In base alle impostazioni definite nella regola AWS Config	Audit Manager recupera la valutazione delle regole direttamente da AWS Config. La valutazione viene importata come prova del controllo di conformità.
AWS Chiamate API	Scatta un'istantanea della configurazione delle risorse direttamente tramite una chiamata API all'indirizzo specificato Servizio AWS.	Giornaliera, settimanale o mensile	Gestione audit effettua la chiamata API in base alla frequenza specificata. La risposta viene importata come prova dei dati di configurazione.

Indipendentemente dalla frequenza di raccolta delle prove, le nuove prove vengono raccolte automaticamente finché la valutazione è attiva. Per ulteriori informazioni, consulta Frequenza di raccolta delle prove.

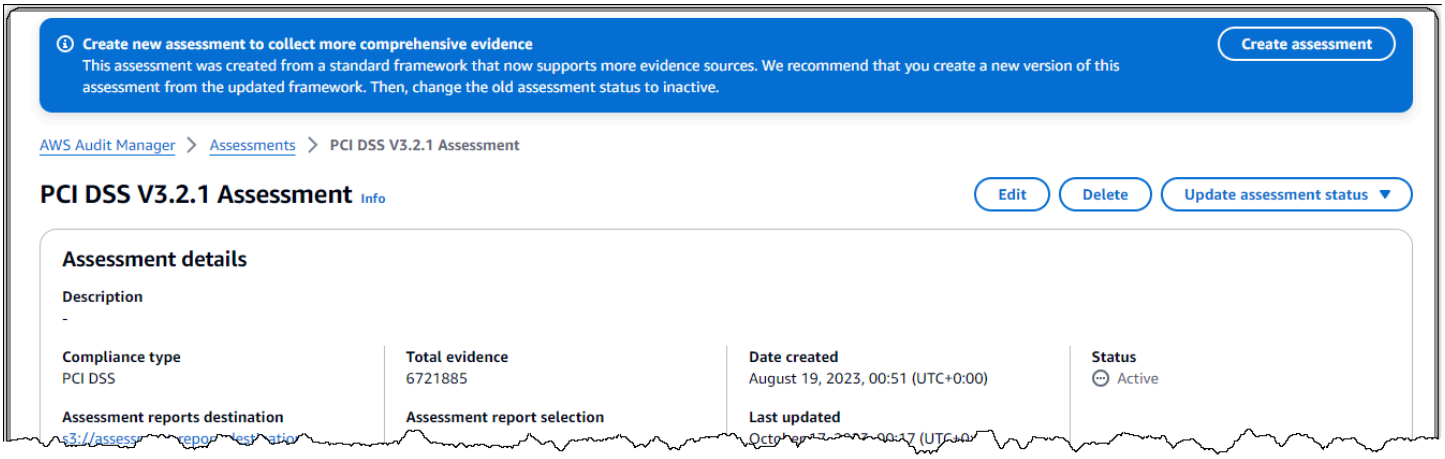
Per ulteriori informazioni, consultare Tipi di fonti di dati supportati per prove automatizzate e Modifica della frequenza con cui un controllo raccoglie le prove.

Ho disabilitato e poi riabilitato Gestione audit e ora le mie valutazioni preesistenti non raccolgono più prove

Quando disabiliti Gestione audit e scegli di non eliminare i tuoi dati, le tue valutazioni esistenti passano a uno stato inattivo e smettono di raccogliere prove. Ciò significa che quando riabiliti Gestione audit, le valutazioni che hai creato in precedenza rimangono disponibili. Tuttavia, non riprendono automaticamente la raccolta delle prove.

Per ricominciare a raccogliere prove per una valutazione preesistente, modifica la valutazione e scegli Salva senza apportare modifiche.

Nella pagina dei dettagli della mia valutazione, mi viene richiesto di ricreare la mia valutazione



Se viene visualizzato un messaggio che dice Crea nuova valutazione per raccogliere prove più complete, significa che Audit Manager ora fornisce una nuova definizione del framework standard da cui è stata creata la valutazione.

Nella nuova definizione del framework, tutti i controlli standard del framework possono ora raccogliere prove da fonti AWS gestite. Ciò significa che ogni volta che viene effettuato un aggiornamento delle

fonti di dati sottostanti per un controllo comune o di base, Audit Manager applica automaticamente lo stesso aggiornamento a tutti i controlli standard correlati.

Per trarre vantaggio da queste fonti AWS gestite, ti consigliamo di creare una nuova valutazione dal framework aggiornato. Dopo aver eseguito questa operazione, puoi modificare lo stato della vecchia valutazione in inattivo. Questa azione aiuta a garantire che la nuova valutazione raccolga le prove più accurate e complete disponibili da fonti AWS gestite. Se non intraprendi alcuna azione, la valutazione continua a utilizzare il vecchio framework e le definizioni di controllo per raccogliere le prove esattamente come faceva prima.

Qual è la differenza tra una fonte di dati e una fonte di prove?

Una fonte di prove determina da dove vengono raccolte le prove. Può trattarsi di una singola fonte di dati o di un raggruppamento predefinito di fonti di dati che si associa a un controllo principale o a un controllo comune.

Una fonte di dati è il tipo di fonte di evidenza più granulare. Una fonte di dati include i seguenti dettagli che indicano all'Audit Manager da dove raccogliere esattamente i dati relativi alle prove:

- Tipo di origine dati (ad esempio, AWS Config)
- Mappatura delle fonti di dati (ad esempio, una AWS Config regola specifica come`s3-bucket-public-write-prohibited`)

La creazione della mia valutazione non è riuscita

Se la creazione della tua valutazione non riesce, potrebbe essere perché hai selezionato troppi Account AWS in ambito di valutazione. Se lo utilizzi AWS Organizations, Audit Manager può supportare fino a 200 account membri nell'ambito di una singola valutazione. Se superi questo numero, la creazione della valutazione potrebbe non riuscire. Come soluzione alternativa, puoi eseguire più valutazioni con account diversi in ambito per ciascuna valutazione.

Cosa succede se rimuovo un account in ambito dalla mia organizzazione?

Quando un account pertinente viene rimosso dall'organizzazione, Gestione audit non raccoglie più prove per quell'account. Tuttavia, l'account continua a comparire nella valutazione sotto la scheda Account AWS. Per rimuovere l'account dall'elenco degli account in ambito, modifica la valutazione. L'account rimosso non viene più visualizzato nell'elenco durante la modifica ed è possibile salvare le modifiche senza includere tale account nell'ambito.

Non riesco a visualizzare i servizi oggetto della mia valutazione

Se non vedi la Servizi AWSscheda, significa che i servizi in questione sono gestiti per te da Audit Manager. Quando crei una nuova valutazione, Audit Manager gestisce i servizi in questione per te da quel momento in poi.

Se hai una valutazione precedente, è possibile che tu abbia già visto questa scheda nella tua valutazione. Tuttavia, Audit Manager rimuove automaticamente questa scheda dalla valutazione e assume la gestione dei servizi inclusi nell'ambito quando si verifica uno dei seguenti eventi:

- Tu modifichi la tua valutazione
- Modifichi uno dei controlli personalizzati utilizzati nella valutazione

Audit Manager deduce i servizi interessati esaminando i controlli di valutazione e le relative fonti di dati e quindi mappando queste informazioni con le corrispondenti. Servizi AWS Se una fonte di dati sottostante cambia per la tua valutazione, aggiorniamo automaticamente l'ambito secondo necessità per riflettere i servizi corretti. Ciò garantisce che la valutazione raccolga prove accurate e complete su tutti i servizi pertinenti del vostro AWS ambiente.

Non riesco a modificare i servizi in ambito per la mia valutazione

Il Modificare una valutazione in AWS Audit Manager flusso di lavoro non ha più una fase di modifica dei servizi. Questo perché Audit Manager ora gestisce Servizi AWS quali rientrano nell'ambito della valutazione.

Se disponi di una valutazione precedente, è possibile che tu abbia definito manualmente i servizi inclusi nell'ambito al momento della creazione di tale valutazione. Tuttavia, non potrai modificare questi servizi in futuro. Audit Manager assume automaticamente la gestione dei servizi oggetto della valutazione quando si verifica uno dei seguenti eventi:

- Tu modifichi la tua valutazione
- Modifichi uno dei controlli personalizzati utilizzati nella valutazione

Audit Manager deduce i servizi interessati esaminando i controlli di valutazione e le relative fonti di dati e quindi mappando queste informazioni con le corrispondenti. Servizi AWS Se una fonte di dati sottostante cambia per la tua valutazione, aggiorniamo automaticamente l'ambito secondo necessità per riflettere i servizi corretti. Ciò garantisce che la valutazione raccolga prove accurate e complete su tutti i servizi pertinenti del vostro AWS ambiente.

Qual è la differenza tra un servizio in ambito e un tipo di origine dati?

A service in scope è Servizio AWS un elemento incluso nell'ambito della valutazione. Quando un servizio è in ambito, Gestione audit raccoglie prove sull'utilizzo di quel servizio e delle sue risorse da parte tua.

> **Note**
>
> Audit Manager gestisce ciò Servizi AWS che rientra nell'ambito delle vostre valutazioni. Se disponi di una valutazione precedente, è possibile che in passato tu abbia specificato manualmente i servizi inclusi nell'ambito. In futuro, non sarà possibile specificare o modificare i servizi inclusi nell'ambito.

Un tipo di origine dati indica da dove vengono raccolte esattamente le prove. Se carichi le tue prove, il tipo di origine dati è Manuale. Se Gestione audit raccoglie le prove, l'origine dati può essere di quattro tipi.

1. AWS Security Hub — Acquisisce un'istantanea del livello di sicurezza delle risorse riportando i risultati del Security Hub.
2. AWS Config — Acquisisce un'istantanea della situazione in materia di sicurezza delle risorse riportando i risultati di. AWS Config
3. AWS CloudTrail — Tiene traccia di un'attività specifica dell'utente per una risorsa.
4. AWS Chiamate API: scatta un'istantanea della configurazione delle risorse direttamente tramite una chiamata API a una specifica Servizio AWS.

Ecco due esempi per illustrare la differenza tra un servizio in ambito e un tipo di origine dati.

Esempio 1

Supponiamo che tu voglia raccogliere prove per un controllo denominato 4.1.2 - Impedisci l'accesso pubblico in scrittura ai bucket S3. Questo controllo verifica i livelli di accesso delle tue policy relative ai bucket S3. Per questo controllo, Audit Manager utilizza una AWS Config regola specifica (s3-bucket-public-write-prohibited) per cercare una valutazione dei bucket S3. In questo esempio, è vero quanto segue:

- service in scopeQuesto è Amazon S3

- Le risorse che vengono valutate sono i tuoi bucket S3
- Il tipo di origine dati è AWS Config
- La mappatura dell'origine dati è una AWS Config regola specifica () `s3-bucket-public-write-prohibited`

Esempio 2

Supponiamo che tu voglia raccogliere prove per un controllo HIPAA denominato 164.308(a)(5)(ii)(C). Questo controllo richiede una procedura di monitoraggio per rilevare accessi inappropriati. Per questo controllo, Audit Manager utilizza CloudTrail i log per cercare tutti gli eventi di accesso alla AWS Management Console. In questo esempio, è vero quanto segue:

- Questo service in scope è IAM
- Le risorse che vengono valutate sono i tuoi utenti
- Il tipo di origine dati è CloudTrail
- La mappatura dell'origine dati è un CloudTrail evento specifico () `ConsoleLogin`

Risoluzione dei problemi relativi ai report di valutazione

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti i report di valutazione in Gestione audit.

Argomenti

Il report di valutazione non è stato generato

Il tuo report di valutazione potrebbe non essere stato generato per una serie di motivi. Puoi iniziare a risolvere il problema controllando le cause più frequenti. Utilizza il seguente elenco di controllo per iniziare.

1. Controlla se alcune delle tue Regione AWS informazioni non corrispondono:
   a. La Regione AWS chiave gestita dal cliente corrisponde Regione AWS alla tua valutazione?

      Se hai fornito la tua chiave KMS per la crittografia dei dati Audit Manager, la chiave deve corrispondere alla tua valutazione. Regione AWS Per risolvere questo problema, modifica la chiave KMS con una che si trovi nella stessa regione della tua valutazione. Per istruzioni su come modificare la chiave KMS, consulta. Configurazione delle impostazioni di crittografia dei dati

   b. La chiave Regione AWS gestita dal cliente corrisponde a quella Regione AWS del bucket S3?

      Se hai fornito la tua chiave KMS per la crittografia dei dati Audit Manager, la chiave deve trovarsi nello stesso Regione AWS bucket S3 che usi come destinazione del rapporto di valutazione. Per risolvere il problema, puoi modificare la chiave KMS o il bucket S3 in modo che si trovino entrambi nella stessa regione della tua valutazione. Per istruzioni su come modificare la chiave KMS, consulta. Configurazione delle impostazioni di crittografia dei dati Per istruzioni su come cambiare il bucket S3, consulta. Configurazione della destinazione predefinita del rapporto di valutazione
2. Controlla le autorizzazioni del bucket S3 che stai utilizzando come destinazione del report di valutazione:
   a. L'entità IAM che genera il report di valutazione dispone delle autorizzazioni necessarie per il bucket S3?

      L'entità IAM deve disporre delle autorizzazioni necessarie per il bucket S3 per pubblicare report in quel bucket. Di seguito proponiamo un esempio di policy che puoi utilizzare.

   b. Il bucket S3 dispone di una policy relativa ai bucket che richiede la crittografia lato server (SSE) tramite SSE-KMS?

      In caso affermativo, la chiave KMS utilizzata in quella policy del bucket deve corrispondere alla chiave KMS specificata nelle impostazioni di crittografia dei dati di Gestione audit. Se non hai configurato una chiave KMS nelle impostazioni di Gestione audit e la tua policy del bucket S3 richiede SSE, assicurati che la policy del bucket consenta SSE-S3. Per istruzioni su come

modificare la chiave KMS, consulta. Configurazione delle impostazioni di crittografia dei dati Per istruzioni su come cambiare il bucket S3, consulta. Configurazione della destinazione predefinita del rapporto di valutazione

Se non riesci ancora a generare correttamente un report di valutazione, esamina i problemi descritti in questa pagina.

Ho seguito l'elenco di controllo sopra riportato e il mio report di valutazione non è ancora stato generato

Gestione audit limita la quantità di prove che è possibile aggiungere a un report di valutazione. Il limite si basa sulla valutazione, sulla regione Regione AWS del bucket S3 utilizzata come destinazione del rapporto di valutazione e sul fatto che la valutazione utilizzi o meno un oggetto gestito dal cliente. AWS KMS key

1. Il limite è di 22.000 per i report della stessa regione (in cui il bucket S3 e la valutazione sono nella stessa Regione AWS).
2. Il limite è di 3.500 per i report interregionali (in cui il bucket S3 e la valutazione sono in Regioni AWS differenti).
3. Il limite è 3.500 se la valutazione utilizza una chiave KMS gestita dal cliente.

Il tentativo di generare un report contenente un numero maggiore di prove di quello stabilito potrebbe impedire lo svolgimento dell'operazione.

Come soluzione alternativa, è possibile generare più report di valutazione anziché un report di valutazione più grande. In questo modo, puoi esportare le prove della tua valutazione in batch di dimensioni più gestibili.

Ricevo un errore di accesso negato quando provo a generare un report

Riceverai un errore `access denied` se la valutazione è stata creata dall'account di un amministratore delegato a cui non appartiene la chiave KMS specificata nelle impostazioni di Gestione audit. Per evitare questo errore, quando designi un amministratore delegato per Gestione audit, assicurati che il suo account abbia accesso alla chiave KMS che hai fornito durante la configurazione di Gestione audit.

Potresti ricevere un errore `access denied` anche se non disponi delle autorizzazioni di scrittura per il bucket S3 che stai utilizzando come destinazione del report di valutazione.

Se ricevi un errore `access denied` accertati di soddisfare i seguenti requisiti:

- La chiave KMS nelle tue impostazioni di Gestione audit fornisce le autorizzazioni all'amministratore delegato. Per la configurazione, segui le istruzioni in Consentire agli utenti di altri account di utilizzare una chiave KMS nella Guida per gli sviluppatori di AWS Key Management Service . Per istruzioni su come rivedere e modificare le impostazioni di crittografia in Audit Manager, vedereConfigurazione delle impostazioni di crittografia dei dati.
- Hai una policy di autorizzazioni che ti garantisce l'accesso in scrittura per il bucket S3 che stai utilizzando come destinazione del report di valutazione. Più specificamente, la tua policy delle autorizzazioni contiene un'azione `s3:PutObject`, specifica l'ARN del bucket S3 e include la chiave KMS utilizzata per crittografare i report di valutazione. Per un esempio di politica utilizzabile, consultaEsempio 2 (autorizzazioni di destinazione del rapporto di valutazione).

> **Note**
>
> Se modifichi le impostazioni di crittografia dei dati di Gestione audit, queste modifiche si applicano a tutte le nuove valutazioni che crei da quel momento in avanti. Ciò include tutti i report di valutazione che crei a partire dalle nuove valutazioni.
> Le modifiche non si applicano alle valutazioni esistenti che hai creato prima di modificare le impostazioni di crittografia. Ciò include nuovi report di valutazione creati a partire da valutazioni esistenti, oltre ai report di valutazione esistenti. Le valutazioni esistenti, con tutti i relativi report di valutazione, continuano a utilizzare la vecchia chiave KMS. Se l'identità IAM che genera il report di valutazione non dispone delle autorizzazioni per utilizzare la vecchia chiave KMS, puoi concedere le autorizzazioni a livello di policy della chiave.

Non riesco a decomprimere il report di valutazione

Se non riesci a decomprimere il report di valutazione in Windows, è probabile che Windows Explorer non sia in grado di estrarlo perché il percorso del file contiene diverse cartelle annidate o nomi lunghi. Questo perché, nel sistema di denominazione dei file di Windows, il percorso della cartella, il nome del file e l'estensione del file non possono superare i 259 caratteri. In caso contrario, si verifica un errore `Destination Path Too Long`.

Per risolvere il problema, prova a spostare il file compresso nella cartella principale della posizione corrente. Puoi quindi riprovare a decomprimerlo da lì. In alternativa, puoi anche provare ad

abbreviare il nome del file compresso o a estrarlo in una posizione diversa con un percorso di file più breve.

Quando scelgo il nome di una prova in un report, non vengo reindirizzato ai dettagli della prova

Questo problema può verificarsi se interagisci con il report di valutazione in un browser o utilizzi il lettore PDF predefinito installato sul tuo sistema operativo. Alcuni lettori PDF predefiniti del browser e del sistema non consentono l'apertura di collegamenti correlati. Ciò significa che, sebbene i collegamenti ipertestuali possano funzionare all'interno del PDF di riepilogo del report di valutazione (ad esempio i nomi dei controlli con collegamenti ipertestuali nel sommario), i collegamenti ipertestuali vengono ignorati quando si tenta di passare dal PDF di riepilogo della valutazione a un PDF separato con i dettagli delle prove.

Se riscontri questo problema, ti consigliamo di utilizzare un lettore PDF dedicato per interagire con i report di valutazione. Per un'esperienza affidabile, ti consigliamo di installare e utilizzare Adobe Acrobat Reader, che puoi scaricare dal sito web di Adobe. Sono disponibili anche altri lettori PDF, ma è stato dimostrato che Adobe Acrobat Reader funziona in modo coerente e affidabile con i report di valutazione di Gestione audit.

La generazione del mio report di valutazione è bloccata nello stato In corso e non so come ciò influisca sulla mia fatturazione

La generazione di report di valutazione non ha alcun impatto sulla fatturazione. La fattura ti viene addebitata solo in base alle prove raccolte dalle tue valutazioni. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Audit Manager.

Risorse aggiuntive

Le pagine seguenti contengono linee guida per la risoluzione dei problemi relativi alla generazione di un report di valutazione da Evidence Finder:

- Non riesco a generare più report di valutazione dai miei risultati di ricerca
- Non posso includere prove specifiche dai miei risultati di ricerca
- Non tutti i risultati del mio Evidence Finder sono inclusi nel report di valutazione
- Desidero generare un report di valutazione dai risultati della mia ricerca, ma la mia istruzione query non riesce

Risoluzione dei problemi relativi ai controlli e ai set di controlli

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti i controlli in Gestione audit.

Problemi generali

- Non riesco a vedere alcun controllo o set di controlli nella mia valutazione
- Non riesco a caricare prove manuali su un controllo
- Cosa significa se un controllo riporta la dicitura «Sostituzione disponibile»?

Problemi di integrazione di AWS Config

- Devo usare più AWS Config regole come fonte di dati per un singolo controllo
- L'opzione delle regole personalizzate non è disponibile quando configuro un'origine dati di controllo
- L'opzione delle regole personalizzate è disponibile, ma nell'elenco a discesa non viene visualizzata alcuna regola
- Sono disponibili alcune regole personalizzate, ma non riesco a vedere la regola che voglio usare
- Non riesco a vedere la regola gestita che voglio usare
- Voglio condividere un framework personalizzato, ma ha controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?
- Cosa succede quando una regola personalizzata viene aggiornata in AWS Config? Devo intraprendere qualche azione in Gestione audit?

Non riesco a vedere alcun controllo o set di controlli nella mia valutazione

In breve, per visualizzare i controlli di una valutazione, devi essere indicato come proprietario dell'audit per quella valutazione. Inoltre, devi avere le autorizzazioni IAM necessarie per visualizzare e gestire le relative risorse di Gestione audit.

Se hai bisogno di accedere ai controlli di una valutazione, chiedi a uno dei proprietari dell'audit incaricato della valutazione di indicarti come proprietario dell'audit. Puoi specificare i proprietari dell'audit quando crei o modifichi una valutazione.

Assicurati inoltre di disporre delle autorizzazioni necessarie per gestire la valutazione. Consigliamo ai titolari delle verifiche di utilizzare la AWSAuditManagerAdministratorAccesspolicy. Per ulteriore

assistenza con le autorizzazioni IAM, contatta l'amministratore o il Supporto AWS. Per informazioni su come allegare una policy IAM a un'identità IAM, consulta Aggiunta di autorizzazioni a un utente e Aggiunta e rimozione di identità IAM nella Guida per l'utente IAM.

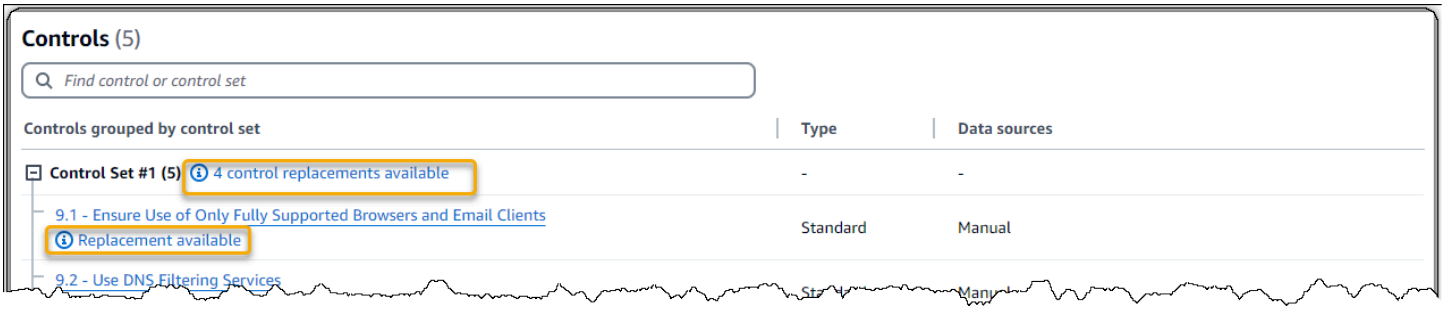
Non riesco a caricare prove manuali su un controllo

Se non riesci a caricare manualmente le prove su un controllo, è probabile che lo stato del controllo sia Inattivo.

Per caricare prove manuali, devi prima modificare lo stato del controllo impostandolo su In fase di revisione o Revisionato. Per istruzioni, consulta Modifica dello stato di un controllo di valutazione in AWS Audit Manager.

> **Important**
>
> Ciascuno Account AWS può caricare manualmente fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera causa il fallimento di qualsiasi altro caricamento manuale per quel controllo. Se devi caricare una grande quantità di prove manuali su un unico controllo, caricale in batch nell'arco di diversi giorni.

Cosa significa se un controllo riporta la dicitura «Sostituzione disponibile»?



Se vedi questo messaggio, significa che è disponibile una definizione di controllo aggiornata per uno o più controlli standard nel tuo framework personalizzato. Ti consigliamo di sostituire questi controlli in modo da poter trarre vantaggio dalle migliori fonti di evidenza ora fornite da Audit Manager.

Per istruzioni su come procedere, vedereNella pagina dei dettagli del mio framework personalizzato, mi viene richiesto di ricreare il mio framework personalizzato.

Devo usare più AWS Config regole come fonte di dati per un singolo controllo

Puoi utilizzare una combinazione di regole gestite e regole personalizzate per un singolo controllo. Per fare ciò, definisci più fonti di evidenza per il controllo e seleziona il tipo di regola preferito per ognuna di esse. Puoi definire fino a 100 fonti di dati gestite dal cliente per un singolo controllo personalizzato.

L'opzione delle regole personalizzate non è disponibile quando configuro un'origine dati di controllo

Ciò significa che non disponi delle autorizzazioni per visualizzare le regole personalizzate per il tuo Account AWS o per la tua organizzazione. Più specificamente, non disponi delle autorizzazioni per eseguire l'DescribeConfigRulesoperazione nella console Audit Manager.

Per risolvere questo problema, contatta l' AWS amministratore per ricevere assistenza. Se sei un amministratore AWS , puoi fornire le autorizzazioni ai tuoi utenti o gruppi gestendo le tue policy IAM.

L'opzione delle regole personalizzate è disponibile, ma nell'elenco a discesa non viene visualizzata alcuna regola

Ciò significa che nessuna regola personalizzata è abilitata e disponibile per l'uso nel tuo Account AWS o nella tua organizzazione.

Se non hai ancora regole personalizzate AWS Config, puoi crearne una. Per istruzioni, consulta AWS Config Regole personalizzate nella Guida per gli sviluppatori di AWS Config .

Se ti aspetti di vedere una regola personalizzata, controlla il seguente elemento di risoluzione dei problemi.

Sono disponibili alcune regole personalizzate, ma non riesco a vedere la regola che voglio usare

Se non riesci a visualizzare la regola personalizzata che prevedi di trovare, ciò potrebbe essere dovuto a uno dei seguenti problemi.

Il tuo account è escluso dalla regola

- È possibile che l'account di amministratore delegato che stai utilizzando sia escluso dalla regola.

L'account di gestione dell'organizzazione (o uno degli account amministratore AWS Config delegato) può creare regole di organizzazione personalizzate utilizzando AWS Command Line Interface (AWS CLI). Quando lo fanno, possono specificare un elenco di account da escludere dalla regola. Se il tuo account è in questo elenco, la regola non è disponibile in Gestione audit.

Per risolvere questo problema, contatta l' AWS Config amministratore per ricevere assistenza. Se sei un AWS Config amministratore, puoi aggiornare l'elenco degli account esclusi eseguendo il put-organization-config-rulecomando.

La regola non è stata creata né abilitata correttamente in AWS Config

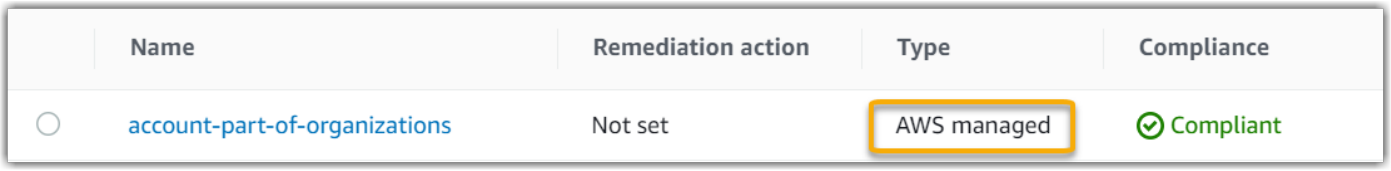
È anche possibile che la regola personalizzata non sia stata creata né abilitata correttamente. Se si è verificato un errore durante la creazione della regola o la regola non è abilitata, non viene visualizzata nell'elenco delle regole disponibili in Gestione audit.

Per ricevere assistenza su questo problema, ti consigliamo di contattare l'amministratore AWS Config .

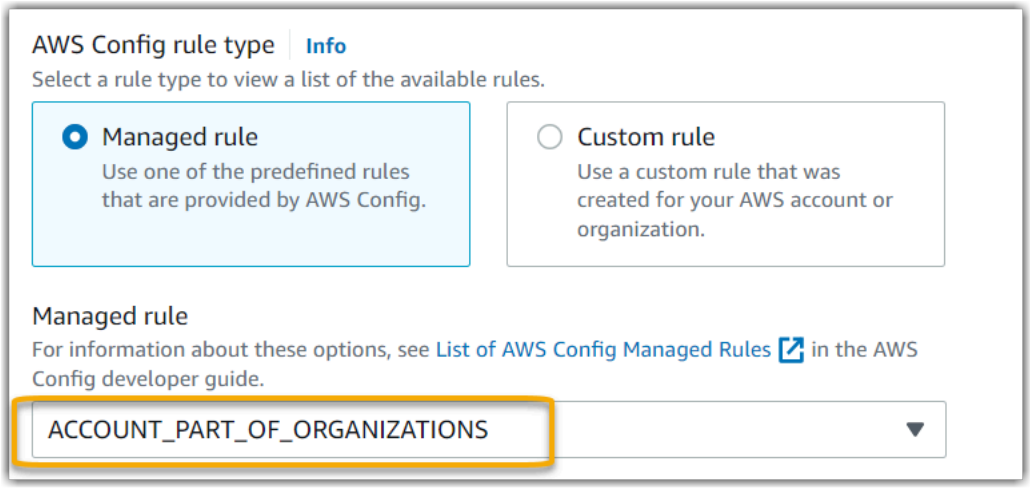
La regola è una regola gestita

Se non riesci a trovare la regola che stai cercando nell'elenco a discesa delle regole personalizzate, è possibile che si tratti di una regola gestita.

Puoi utilizzare la console AWS Configper verificare se una regola è una regola gestita. Dal menu di navigazione a sinistra, scegli Regole e cerca la regola nella tabella. Se la regola è una regola gestita, la colonna Tipo mostra AWS gestita.

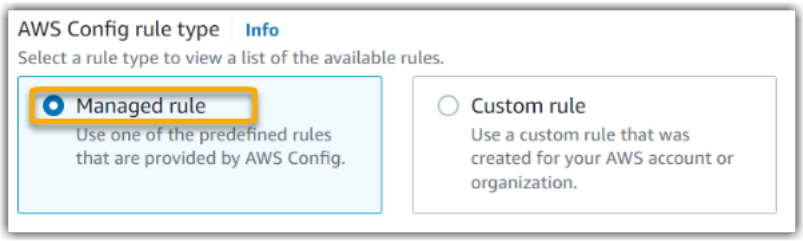


Dopo aver confermato che si tratta di una regola gestita, torna in Gestione audit e seleziona Regola gestita come tipo di regola. Quindi, cerca la parola chiave di identificazione della regola gestita nell'elenco a discesa delle regole gestite.



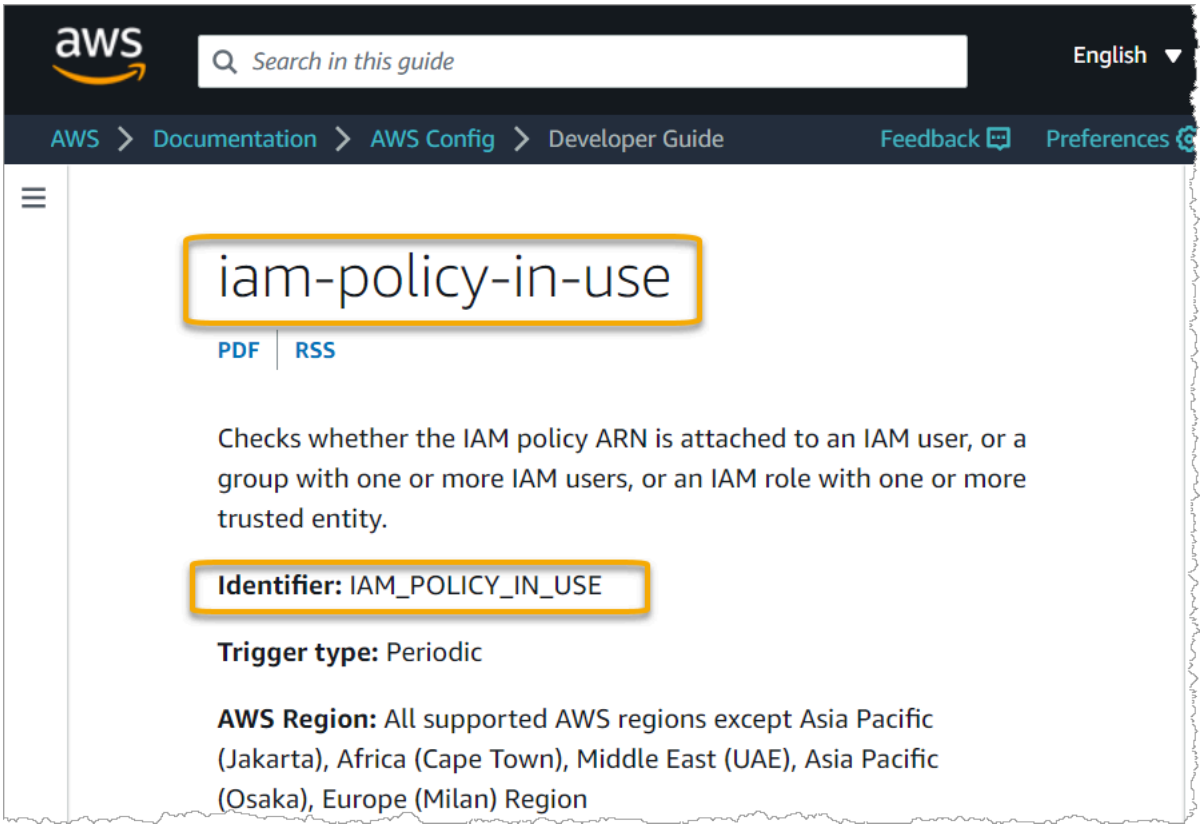
Non riesco a vedere la regola gestita che voglio usare

Prima di selezionare una regola dall'elenco a discesa nella console di Gestione audit, assicurati di aver selezionato Regola gestita come tipo di regola.

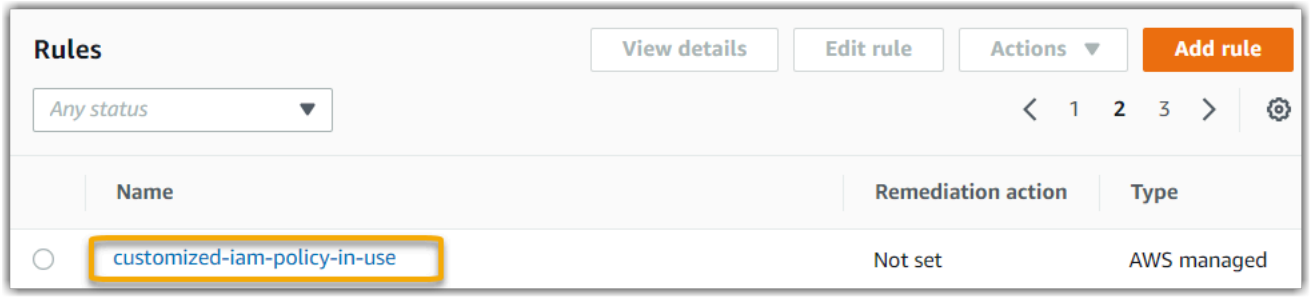


Se ancora non riesci a visualizzare la regola gestita che ti aspetti di trovare, è possibile che tu stia cercando il nome della regola. Devi invece cercare l'identificatore della regola.

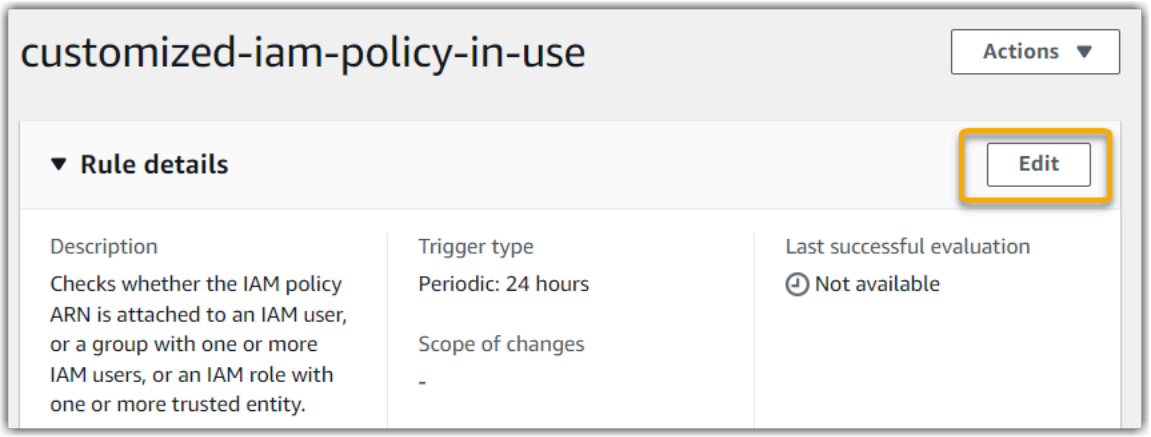
Se utilizzi una regola gestita predefinita, il nome e l'identificatore sono simili. Il nome è in minuscolo e utilizza trattini (ad esempio, `iam-policy-in-use`). L'identificatore è in maiuscolo e utilizza caratteri di sottolineatura (ad esempio, `IAM_POLICY_IN_USE`). Per trovare l'identificatore di una regola gestita predefinita, consulta l'elenco delle parole chiave supportate per le regole AWS Config gestite e segui il link relativo alla regola che desideri utilizzare. Verrai reindirizzato alla AWS Config documentazione relativa a quella regola gestita. Da qui è possibile visualizzare sia il nome sia l'identificatore. Cerca la parola chiave identificativa nell'elenco a discesa di Gestione audit.



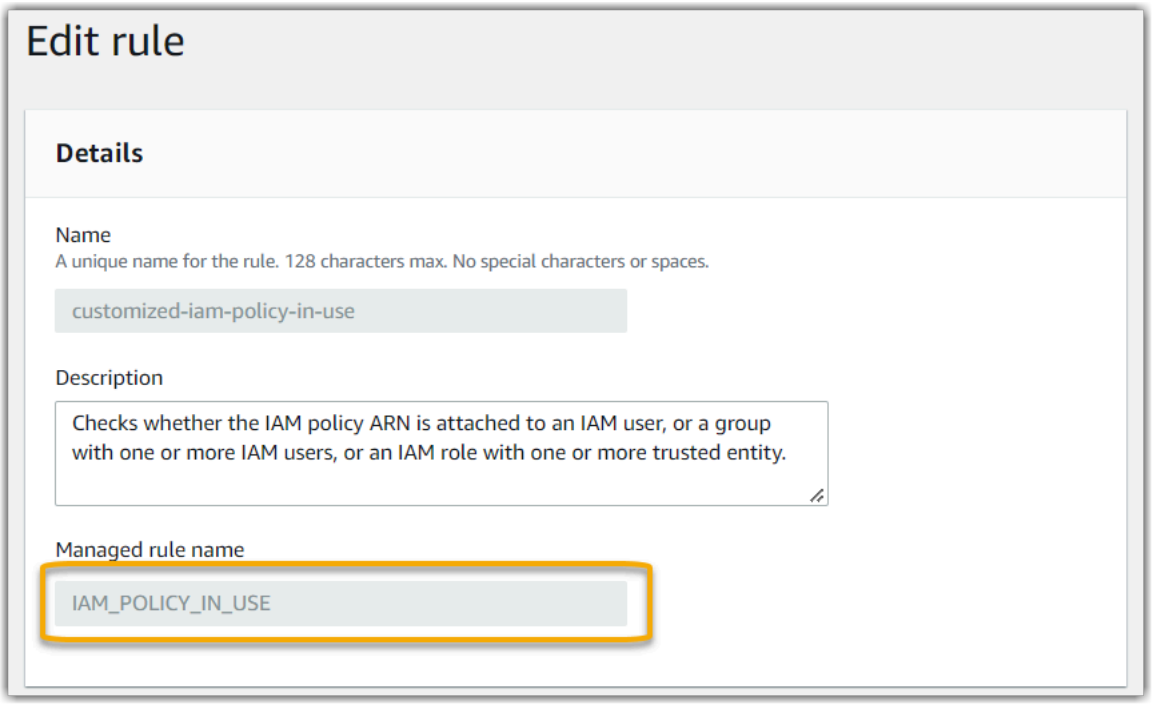
Se utilizzi una regola gestita personalizzata, puoi utilizzare la AWS Config console per trovare l'identificatore della regola. Ad esempio, supponiamo che tu voglia utilizzare la regola gestita chiamata `customized-iam-policy-in-use`. Per trovare l'identificatore per questa regola, vai alla AWS Config console, scegli Regole nel menu di navigazione a sinistra e scegli la regola nella tabella.



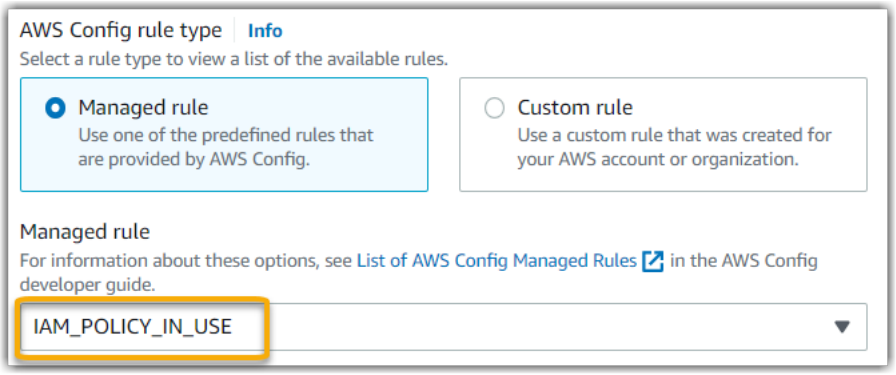
Scegli Modifica per aprire i dettagli sulla regola gestita.



Nella sezione Dettagli, puoi trovare l'identificatore di origine da cui è stata creata la regola gestita (`IAM_POLICY_IN_USE`).



È ora possibile tornare alla console di Gestione audit e selezionare la stessa parola chiave identificativa dall'elenco a discesa.



Voglio condividere un framework personalizzato, ma ha controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?

Sì, il destinatario può raccogliere prove per questi controlli, ma a tal fine sono necessari alcuni passaggi.

Affinché Audit Manager raccolga prove utilizzando una AWS Config regola come mappatura dell'origine dati, deve essere vero quanto segue. Questo vale sia per le regole gestite sia per le regole personalizzate.

1. La regola deve esistere nell'ambiente del destinatario AWS
2. La regola deve essere abilitata nell' AWS ambiente del destinatario

Ricorda che le AWS Config regole personalizzate del tuo account probabilmente non esistono già nell' AWS ambiente del destinatario. Inoltre, quando il destinatario accetta la richiesta di condivisione, Gestione audit non ricrea nessuna delle tue regole personalizzate nel suo account. Affinché il destinatario possa raccogliere prove utilizzando le tue regole personalizzate come mappatura dell'origine dati, deve creare le stesse regole personalizzate nella sua istanza di AWS Config. Dopo che il destinatario ha creato e quindi abilitato le regole, Gestione audit può raccogliere prove da tale origine dati.

Consigliamo di comunicare con il destinatario per fargli sapere se è necessario creare regole personalizzate per la sua istanza di AWS Config.

Cosa succede quando una regola personalizzata viene aggiornata in AWS Config? Devo intraprendere qualche azione in Gestione audit?

Per gli aggiornamenti delle regole all'interno del tuo ambiente AWS

Se si aggiorna una regola personalizzata all'interno del proprio AWS ambiente, non è necessaria alcuna azione in Audit Manager. Gestione audit rileva e gestisce gli aggiornamenti delle regole come descritto nella tabella seguente. Gestione audit non invia notifiche quando rileva un aggiornamento delle regole.

Scenario	Cosa fa Gestione audit	Cosa devi fare tu
Una regola personalizzata viene aggiornata nell'istanza di AWS Config	Gestione audit continua a segnalare gli esiti di quella regola utilizzando la definizio ne di regola aggiornata.	Non è richiesta alcuna azione.
Una regola personalizzata viene eliminata nell'istanza di AWS Config	Gestione audit interrompe la segnalazione degli esiti della regola eliminata.	Non è richiesta alcuna azione. Se lo desideri, puoi modificar e i controlli personalizzati che utilizzavano la regola eliminata come mappatura dell'orig ine dati. In questo modo puoi ripulire le impostazioni dell'orig ine dati rimuovendo la regola eliminata. In caso contrario, il nome della regola eliminata rimane come una mappatura dell'origine dati inutilizzata.

Per gli aggiornamenti delle regole al di fuori AWS dell'ambiente

Se una regola personalizzata viene aggiornata al di fuori dell' AWS ambiente, Audit Manager non rileva l'aggiornamento della regola. Questo è un aspetto da considerare se si utilizzano framework personalizzati condivisi. Questo perché, in questo scenario, il mittente e il destinatario lavorano

ciascuno in AWS ambienti separati. La tabella seguente indica le azioni consigliate per questo scenario.

Il tuo ruolo	Scenario	Azione consigliata
Mittent	• Hai condiviso un framework che utilizza regole personalizzate come mappatura dell'origine dati. • Dopo aver condiviso il framework, hai aggiornato o eliminato una di queste regole in AWS Config.	Informa il destinatario del tuo aggiornamento. In questo modo, potrà applicare lo stesso aggiornamento e rimanere sincronizzato con l'ultima definizione della regola.
Destina rio	• Hai accettato un framework condiviso che utilizza regole personalizzate come mappatura dell'origine dati. • Dopo aver ricreato le regole personalizzate nell'istanza di AWS Config, il mittente ha aggiornato o eliminato una di tali regole.	Aggiorna la regola corrispondente nella tua istanza di AWS Config.

Risoluzione dei problemi della dashboard

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti la dashboard di Gestione audit.

Argomenti

Non ci sono dati nella mia dashboard

Se i numeri nel Snapshot giornaliero widget mostrano un trattino (-), ciò indica che non sono disponibili dati. È necessario che sia presente almeno una valutazione attiva per visualizzare i dati nella dashboard. Per iniziare, crea una valutazione. Dopo un periodo di 24 ore, i dati della tua valutazione inizieranno a comparire nella dashboard.

> **Note**
>
> Se i numeri nel widget di snapshot giornaliero sono accompagnati da uno zero (0), significa che le valutazioni attive (o la valutazione selezionata) non hanno prove non conformi.

Non riesco più a visualizzare i dati del dashboard per la mia valutazione

Audit Manager non visualizza i dati del dashboard per le valutazioni create utilizzando la vecchia versione dei framework standard. È possibile risolvere questo problema ricreando la valutazione dall'ultima versione del framework standard.

Quando Audit Manager ha lanciato la libreria Common Controls il 6 giugno 2024, abbiamo aggiornato tutti i framework standard. Nelle nuove definizioni del framework, tutti i controlli standard del framework possono ora raccogliere prove da s. AWS managed source Ciò significa che ogni volta che viene effettuato un aggiornamento delle fonti di dati sottostanti per un controllo comune o di base, Audit Manager applica automaticamente lo stesso aggiornamento a tutti i controlli standard correlati.

Non è necessario creare una nuova valutazione ogni volta che queste mappature delle fonti di dati vengono aggiornate automaticamente. La creazione di una nuova valutazione è un'attività unica che ti consigliamo di completare dopo il lancio di Common Controls.

Per visualizzare i dati approfonditi sulla dashboard in futuro, crea una nuova valutazione dalla versione aggiornata del framework standard. Dopo aver creato la nuova valutazione, puoi modificare lo stato della vecchia valutazione in inattiva.

L'opzione di download in formato CSV non è disponibile

Questa opzione è disponibile solo per le valutazioni individuali. Assicurati di aver applicato un Filtro di valutazione alla dashboard, quindi riprova. Tieni presente che puoi scaricare un solo file CSV alla volta.

Non vedo il file scaricato quando cerco di scaricare un file CSV

Se un dominio di controllo contiene un numero elevato di controlli, potrebbe verificarsi un breve ritardo durante la generazione del file CSV da parte di Gestione audit. Dopo la generazione, il file viene scaricato automaticamente.

Se continui a non visualizzare il file scaricato, assicurati che la tua connessione Internet funzioni normalmente e che tu stia utilizzando la versione più recente del tuo browser web. Inoltre, controlla la cartella dei download recenti. I file vengono scaricati nella posizione predefinita determinata dal browser. Se il problema persiste, prova a scaricare il file utilizzando un altro browser.

Nella dashboard non è presente un controllo o un dominio di controllo specifico

Ciò significa probabilmente che le tue valutazioni attive (o la valutazione specificata) non contengono dati pertinenti per quel controllo o dominio di controllo.

Un dominio di controllo viene visualizzato nella dashboard solo se sono soddisfatti i due criteri seguenti:

- Le tue valutazioni attive (o la valutazione specificata) contengono almeno un controllo correlato a quel dominio
- Almeno un controllo all'interno di quel dominio ha raccolto prove nella data riportata nella parte superiore della dashboard

Un controllo viene visualizzato all'interno di un dominio solo se ha raccolto prove nella data riportata nella parte superiore della dashboard.

Lo snapshot quotidiano mostra ogni giorno quantità diverse di prove. È normale che sia così?

Non tutte le prove vengono raccolte su base giornaliera. I controlli nelle valutazioni di Gestione audit sono mappati a diverse origini dati e ognuno può avere un programma di raccolta delle prove diverso. Di conseguenza, è previsto che lo snapshot giornaliero mostri una quantità variabile di prove ogni giorno. Per ulteriori informazioni, consulta Frequenza di raccolta delle prove.

Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti gli amministratori delegati in Gestione audit.

Argomenti

Non riesco a configurare Gestione audit con il mio account di amministratore delegato

Sebbene siano supportati più amministratori delegati AWS Organizations, Audit Manager consente un solo amministratore delegato. Se si tenta di designare più amministratori delegati in Gestione audit, viene visualizzato il seguente messaggio di errore:

- Console: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Scegli l'account individuale che desideri utilizzare come amministratore delegato in Gestione audit. Assicurati di registrare prima l'account di amministratore delegato in Organizations, quindi aggiungi lo stesso account come amministratore delegato in Gestione audit.

Quando creo una valutazione, non riesco a visualizzare gli account della mia organizzazione in Account in ambito

Se desideri che la valutazione di Gestione audit includa più account della tua organizzazione, devi specificare un amministratore delegato.

Assicurati di aver configurato un account di amministratore delegato per Gestione audit. Per istruzioni, consulta Aggiungere un amministratore delegato.

Alcune questioni da tenere a mente:

- Non puoi utilizzare il tuo account di AWS Organizations gestione come amministratore delegato in Audit Manager.
- Se si desidera abilitare Audit Manager in più di una regione Regione AWS, è necessario designare un account amministratore delegato separatamente in ciascuna regione. Nelle impostazioni di Gestione audit, designa lo stesso account di amministratore delegato in tutte le regioni.
- Quando designi un amministratore delegato, assicurati che il suo account abbia accesso alla chiave KMS che fornisci durante la configurazione di Gestione audit. Per informazioni su come rivedere e modificare le impostazioni di crittografia, consulta. Configurazione delle impostazioni di crittografia dei dati

Ricevo un errore di accesso negato quando provo a generare un report di valutazione utilizzando il mio account di amministratore delegato

Riceverai un errore `access denied` se la valutazione è stata creata dall'account di un amministratore delegato a cui non appartiene la chiave KMS specificata nelle impostazioni di Gestione audit. Per evitare questo errore, quando designi un amministratore delegato per Gestione audit, assicurati che il suo account abbia accesso alla chiave KMS che hai fornito durante la configurazione di Gestione audit.

Potresti ricevere un errore `access denied` anche se non disponi delle autorizzazioni di scrittura per il bucket S3 che stai utilizzando come destinazione del report di valutazione.

Se ricevi un errore `access denied` accertati di soddisfare i seguenti requisiti:

- La chiave KMS nelle tue impostazioni di Gestione audit fornisce le autorizzazioni all'amministratore delegato. Per la configurazione, segui le istruzioni in Consentire agli utenti di altri account di utilizzare una chiave KMS nella Guida per gli sviluppatori di AWS Key Management Service

. Per istruzioni su come rivedere e modificare le impostazioni di crittografia in Audit Manager, vedereConfigurazione delle impostazioni di crittografia dei dati.

- Hai una policy di autorizzazioni che ti garantisce l'accesso in scrittura alla destinazione del report di valutazione. Più specificamente, la tua policy delle autorizzazioni contiene un'azione `s3:PutObject`, specifica l'ARN del bucket S3 e include la chiave KMS utilizzata per crittografare i report di valutazione. Per un esempio di politica utilizzabile, consultaEsempio 2 (autorizzazioni di destinazione del rapporto di valutazione).

> **Note**
>
> Se modifichi le impostazioni di crittografia dei dati di Gestione audit, queste modifiche si applicano a tutte le nuove valutazioni che crei da quel momento in avanti. Ciò include tutti i report di valutazione che crei a partire dalle nuove valutazioni.
> Le modifiche non si applicano alle valutazioni esistenti che hai creato prima di modificare le impostazioni di crittografia. Ciò include nuovi report di valutazione creati a partire da valutazioni esistenti, oltre ai report di valutazione esistenti. Le valutazioni esistenti, con tutti i relativi report di valutazione, continuano a utilizzare la vecchia chiave KMS. Se l'identità IAM che genera il report di valutazione non dispone delle autorizzazioni per utilizzare la vecchia chiave KMS, puoi concedere le autorizzazioni a livello di policy della chiave.

Cosa succede in Gestione audit se scollego un account membro dalla mia organizzazione?

Quando si scollega un account membro da un'organizzazione, Gestione audit riceve una notifica relativa a questo evento. Gestione audit rimuove quindi automaticamente tale Account AWS dall'elenco degli account in ambito delle valutazioni esistenti. Quando specifichi l'ambito delle nuove valutazioni, l'account scollegato non appare più nell'elenco degli Account AWS idonei.

Quando Gestione audit rimuove un account membro non collegato dagli elenchi degli account in ambito delle tue valutazioni, non ricevi alcuna notifica di questa modifica. Inoltre, all'account membro non collegato non viene notificato che Gestione audit non è più abilitato sul suo account.

Cosa succede se ricollego un account membro alla mia organizzazione?

Quando ricolleghi un account membro alla tua organizzazione, quell'account non viene aggiunto automaticamente all'ambito delle tue valutazioni esistenti di Gestione audit. Tuttavia, l'account

membro ricollegato ora appare come idoneo Account AWS quando si specificano gli account nell'ambito delle valutazioni.

- Per le valutazioni esistenti, puoi modificare manualmente l'ambito della valutazione per aggiungere l'account membro ricollegato. Per istruzioni, consulta Fase 2: Modifica Account AWS l'ambito.
- Per nuove valutazioni, puoi aggiungere l'account ricollegato durante l'impostazione della valutazione. Per istruzioni, consulta Fase 2: Specificare Account AWS l'ambito.

Cosa succede se eseguo la migrazione di un account membro da un'organizzazione all'altra?

Se un account membro ha Gestione audit abilitato nell'organizzazione 1 e poi migra all'organizzazione 2, Gestione audit non sarà abilitato per l'organizzazione 2.

Risoluzione dei problemi in Evidence Finder

Utilizza le informazioni presentate in questa pagina per risolvere i problemi più comuni relativi a Evidence Finder in Gestione audit.

Problemi generali relativi a Evidence Finder

- Non riesco ad abilitare Evidence Finder
- Ho abilitato Evidence Finder, ma non vedo prove precedenti nei risultati di ricerca
- Non riesco a disabilitare Evidence Finder
- La mia query di ricerca non riesce

Problemi relativi ai report di valutazione in Evidence Finder

- Non riesco a generare più report di valutazione dai miei risultati di ricerca
- Non posso includere prove specifiche dai miei risultati di ricerca
- Non tutti i risultati del mio Evidence Finder sono inclusi nel report di valutazione
- Desidero generare un report di valutazione dai risultati della mia ricerca, ma la mia istruzione query non riesce
- Risorse aggiuntive

Problemi di esportazione in formato CSV in Evidence Finder

- La mia esportazione in formato CSV non è riuscita
- Non posso esportare prove specifiche dai miei risultati di ricerca
- Non riesco a esportare più file CSV contemporaneamente

Non riesco ad abilitare Evidence Finder

Alcuni dei motivi comuni per cui non è possibile abilitare Evidence Finder sono:

Non hai le autorizzazioni necessarie

Se stai tentando di abilitare Evidence Finder per la prima volta, assicurati di disporre delle autorizzazioni necessarie per abilitare Evidence Finder. Queste autorizzazioni ti consentono di creare e gestire un archivio dati sugli eventi in CloudTrail Lake, necessario per supportare le query di ricerca di Evidence Finder. Le autorizzazioni consentono inoltre di eseguire query di ricerca in Evidence Finder.

Se hai bisogno di assistenza con le autorizzazioni, contatta il tuo amministratore. AWS Se sei un AWS amministratore, puoi copiare la dichiarazione di autorizzazione richiesta e allegarla a una policy IAM.

Stai utilizzando il tuo account di gestione di Organizations

Tieni presente che non puoi utilizzare il tuo account di gestione per abilitare Evidence Finder. Accedi come account di amministratore delegato e riprova.

In precedenza hai disabilitato Evidence Finder

La riabilitazione di Evidence Finder non è al momento supportata. Se in precedenza hai disabilitato Evidence Finder, non potrai riabilitarlo.

Ho abilitato Evidence Finder, ma non vedo prove precedenti nei risultati di ricerca

Quando abiliti Evidence Finder, sono necessari fino a sette giorni prima che tutti i dati relativi alle prove precedenti siano disponibili.

Durante tale periodo, viene eseguito il backfill di un datastore di eventi con i dati delle prove degli ultimi due anni. Ciò significa che se utilizzi Evidence Finder subito dopo averlo abilitato, non tutti i risultati saranno disponibili fino al completamento del backfill.

Per istruzioni su come verificare lo stato del riempimento dei dati, consultaConferma dello stato di Evidence Finder .

Non riesco a disabilitare Evidence Finder

Questo problema potrebbe essere causato da uno dei seguenti motivi.

Non hai le autorizzazioni necessarie

Se stai cercando di disabilitare Evidence Finder, assicurati di disporre delle autorizzazioni necessarie per disabilitare Evidence Finder. Queste autorizzazioni ti consentono di aggiornare ed eliminare un archivio di dati sugli eventi in CloudTrail Lake, necessario per disabilitare Evidence Finder.

Se hai bisogno di assistenza con le autorizzazioni, contatta il tuo amministratore. AWS Se sei un AWS amministratore, puoi copiare la dichiarazione di autorizzazione richiesta e allegarla a una policy IAM.

È ancora in corso una richiesta per abilitare Evidence Finder

Quando richiedi di abilitare Evidence Finder, creiamo un datastore di eventi per supportare le richieste di Evidence Finder. Non puoi disabilitare Evidence Finder durante la creazione del datastore di eventi.

Per procedere, attendi il completamento della creazione del datastore di eventi e riprova. Per ulteriori informazioni, consulta Conferma dello stato di Evidence Finder .

Hai già richiesto di disabilitare Evidence Finder

Quando richiedi di disabilitare Evidence Finder, eliminiamo il datastore di eventi utilizzato per le query di Evidence Finder. Se riprovi a disabilitare Evidence Finder durante l'eliminazione del datastore di eventi, ricevi un messaggio di errore.

In questo caso, non è necessaria alcuna azione da parte tua. Attendi che il datastore di eventi venga eliminato. Al termine dell'operazione, Evidence Finder viene disabilitato. Per ulteriori informazioni, consulta Conferma dello stato di Evidence Finder .

La mia query di ricerca non riesce

L'insuccesso di una query di ricerca potrebbe essere dovuto a uno dei seguenti motivi.

Non hai le autorizzazioni necessarie

Verifica che l'utente disponga delle autorizzazioni necessarie per eseguire query di ricerca e accedere ai risultati della ricerca. In particolare, sono necessarie le autorizzazioni per le seguenti CloudTrail azioni:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Se hai bisogno di assistenza con le autorizzazioni, contatta l'amministratore AWS . Se sei un AWS amministratore, puoi copiare la dichiarazione di autorizzazione richiesta e allegarla a una policy IAM.

Stai eseguendo il numero massimo di query

È possibile eseguire fino a cinque query alla volta. Se stai eseguendo il numero massimo di query simultanee consentito, si verifica un errore `MaxConcurrentQueriesException`. Se viene visualizzato questo messaggio di errore, attendi un minuto per consentire il completamento di alcune query, quindi esegui nuovamente la query.

L'istruzione di query presenta un errore di convalida

Se utilizzi l'API o la CLI per eseguire l'StartQueryoperazione CloudTrail Lake, assicurati che la tua `queryStatement` sia valida. Se l'istruzione di query presenta errori di convalida, sintassi errata o parole chiave non supportate, il risultato è un `InvalidQueryStatementException`.

Per ulteriori informazioni sulla scrittura di una query, consulta Creare o modificare una query nella Guida per l'utente AWS CloudTrail .

Per esempi di sintassi valida, consulta i seguenti esempi di istruzioni di query che possono essere utilizzate per interrogare un datastore di eventi di Gestione audit.

Esempio 1: analizzare le prove e il relativo stato di conformità

Questo esempio individua le prove con qualsiasi stato di conformità in tutte le valutazioni presenti in un account, entro un intervallo di date specificato.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Esempio 2: determinare la non conformità delle prove relative a un controllo

In questo esempio sono riportate tutte le prove non conformi in un intervallo di date specificato per una valutazione e un controllo specifici.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Esempio 3: contare le prove per nome

Questo esempio elenca le prove totali di valutazione in un intervallo di date specificato, raggruppate per nome e ordinate in base al numero di prove.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Esempio 4: esplorare le prove per origine dati e servizio

In questo esempio sono riportate tutte le prove in un intervallo di date specificato per un'origine dati e un servizio specifici.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Esempio 5: esplorare le prove conformi per origine dati e dominio di controllo

In questo esempio sono riportate le prove conformi di domini di controllo specifici, dove le prove provengono da un'origine dati diversa da AWS Config.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
```

```
monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
Config')
```

Altre eccezioni API

L'StartQueryAPI potrebbe fallire per diversi altri motivi. Per un elenco completo dei possibili errori e descrizioni, consulta StartQuery Errors in the AWS CloudTrail API Reference.

Non riesco a generare più report di valutazione dai miei risultati di ricerca

Questo errore è causato dall'esecuzione di troppe query CloudTrail Lake contemporaneamente.

L'errore può verificarsi se raggruppi i risultati della ricerca e cerchi di generare immediatamente report di valutazione per ogni voce dei risultati raggruppati. Quando ottieni i risultati della ricerca e generi un report di valutazione, ogni azione richiama una query. Puoi eseguire un massimo di cinque query alla volta. Se stai eseguendo il numero massimo di query simultanee consentito, viene restituito un errore `MaxConcurrentQueriesException`.

Per evitare questo errore, assicurati di non generare troppi report di valutazione contemporaneamente. Se stai eseguendo il numero massimo di query simultanee consentito, viene restituito un errore `MaxConcurrentQueriesException`. Se ricevi questo messaggio di errore, attendi qualche minuto per consentire il completamento dei report di valutazione in corso.

Puoi controllare lo stato dei report di valutazione dalla pagina del centro di download nella console di Gestione audit. Una volta che i report sono completati, torna ai risultati raggruppati in Evidence Finder. Potrai continuare a ottenere i risultati e generare un report di valutazione per ogni voce.

Non posso includere prove specifiche dai miei risultati di ricerca

Tutti i risultati della tua ricerca sono inclusi nel report di valutazione. Non puoi aggiungere selettivamente singole righe dal tuo set di risultati di ricerca.

Se nel report di valutazione desideri includere solo risultati di ricerca specifici, ti consigliamo di modificare i filtri di ricerca correnti. Questo ti permetterà di restringere i risultati in modo da individuare solo le prove che desideri includere nel report.

Non tutti i risultati del mio Evidence Finder sono inclusi nel report di valutazione

Quando generi un report di valutazione, ci sono dei limiti alla quantità di prove che puoi aggiungere. Il limite si basa sulla valutazione, sulla regione Regione AWS del bucket S3 utilizzata come destinazione del rapporto di valutazione e sul fatto che la valutazione utilizzi o meno un file gestito dal cliente. AWS KMS key

1. Il limite è di 22.000 per i report della stessa regione (in cui il bucket S3 e la valutazione sono nella stessa Regione AWS).
2. Il limite è di 3.500 per i report interregionali (in cui il bucket S3 e la valutazione sono in Regioni AWS differenti).
3. Il limite è 3.500 se la valutazione utilizza una chiave KMS gestita dal cliente.

Se superi questo limite, il report viene comunque creato. Tuttavia, Gestione audit aggiunge solo i primi 3.500 o 22.000 elementi di prova al report.

Per evitare questo problema, ti consigliamo di modificare i filtri di ricerca correnti. In questo modo, puoi ridurre i risultati della ricerca concentrandoti su una quantità minore di prove. Se necessario, puoi ripetere questo metodo e generare più report di valutazione anziché un report più grande.

Desidero generare un report di valutazione dai risultati della mia ricerca, ma la mia istruzione query non riesce

Se utilizzi l'CreateAssessmentReportAPI e l'istruzione della query restituisce un'eccezione di convalida, consulta la tabella seguente per indicazioni su come risolvere il problema.

> **Note**
>
> Anche se un'istruzione di query funziona CloudTrail, la stessa query potrebbe non essere valida per la generazione di report di valutazione in Audit Manager. Ciò è dovuto ad alcune differenze nella convalida delle query tra i due servizi.

Clausol	Problema	Soluzione	Note
`SELECT`	La clausola `SELECT` contiene un nome di colonna	Rimuovere la clausola `SELECT` e sostituirla con `SELECT eventJson .`	Solo `SELECT eventJson` è supportata. Questa convalida viene gestita da Gestione audit.
`FROM`	La clausola `FROM` contiene un ID del datastore di eventi non valido oppure L'ID del datastore di eventi fornito non corrisponde all'ID del datastore di eventi nelle tue impostazioni di Gestione audit	Rimuovi la clausola `FROM` e sostituiscila con `FROM` *`edsID`*, dove il valore di `edsID` corrisponde all'ID del datastore di eventi specificato nelle impostazioni di Gestione audit. Puoi recuperare l'ARN del datastore di eventi dalle tue impostazioni di Gestione audit. Per ulteriori informazioni, GetSettingsconsulta l'AWS Audit Manager API Reference.	Questa convalida viene gestita da Gestione audit.
`GROUP BY`	Nella query è presente una clausola `GROUP BY`	Rimuovi la clausola `GROUP BY`.	Questa convalida viene gestita da Gestione audit.
`HAVING`	Nella query è presente una clausola `HAVING`	Rimuovi la clausola `HAVING`.	Questa convalida viene gestita da Gestione audit.
`LIMIT`	La clausola `LIMIT` contiene un valore che supera il limite massimo consentito	Se la clausola `LIMIT` esiste, assicurati che il suo valore sia uguale o inferiore al limite massimo supportato: • Per i report relativi alla stessa regione, il limite è 22.000	Nella console, non c'è limite al numero di risultati di prove che possono essere restituiti. Tuttavia, quando si genera un report di valutazione, viene applicato un limite alla quantità di prove che è possibile includere.

Clausol	Problema	Soluzione	Note
		• Per i report interregionali, il limite è 3.500 • Per i report in cui la valutazione correlata utilizza una soluzione gestita dal cliente AWS KMS key, il limite è 3.500	Se non è fornito alcun valore `LIMIT` nell'istruzione di query, vengono applicati i limiti massimi predefiniti. Questa convalida viene gestita da Gestione audit.
`ORDER BY`	La clausola `ORDER BY` contiene funzioni aggregate o alias che non sono presenti nella clausola `SELECT`	Assicurati che la clausola `ORDER BY` non contenga condizioni che utilizzino funzioni aggregate o alias.	Questa convalida è gestita dall'API. CloudTrail StartQuery
`WHERE`	La clausola `WHERE` contiene più di una `assessmentId` oppure La clausola `WHERE` contiene un `assessmentId` che non corrisponde all'`assessmentId` nella tua richiesta `createAssessmentReport` oppure La clausola `WHERE` contiene un nome di colonna non supportato	Assicurati che sia specificato un solo AssessmentID e che corrisponda al parametro AssessmentID specificato nella richiesta API `createAssessmentReport` . Rimuovi i nomi di colonna non supportati.	Questa convalida è gestita dall'API. CloudTrail StartQuery

Esempi

Gli esempi seguenti mostrano come utilizzare il `queryStatement` parametro quando si chiama l'CreateAssessmentReportoperazione. Prima di utilizzare queste query, sostituisci il *testo segnaposto* con i tuoi valori `edsId` e `assessmentId`.

Esempio 1: creazione di un report (si applica il limite della stessa regione)

In questo esempio il report creato include i risultati dei bucket S3 creati tra il 22 e il 23 gennaio 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Esempio 2: creazione di un report (si applica il limite interregionale)

In questo esempio il report creato include tutti i risultati di uno specifico datastore di eventi e valutazioni per il quale non sia stato indicato un intervallo di date.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Esempio 3: creazione di un report (al di sotto del limite predefinito)

In questo esempio il report creato include tutti i risultati di uno specifico datastore di eventi e valutazioni con un limite inferiore al massimo consentito.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Risorse aggiuntive

La pagina seguente contiene indicazioni generali per la risoluzione dei problemi relativi ai report di valutazione:

- Risoluzione dei problemi relativi ai report di valutazione

La mia esportazione in formato CSV non è riuscita

L'esportazione in formato CSV potrebbe non riuscire per una serie di motivi. Puoi risolvere questo problema controllando le cause più frequenti.

Innanzitutto, assicurati di soddisfare i prerequisiti per l'utilizzo della funzionalità di esportazione CSV:

Hai abilitato con successo Evidence Finder

Se non hai abilitato Evidence Finder, non puoi eseguire una query di ricerca ed esportare i risultati della ricerca.

Il backfill del datastore di prove è completo

Se utilizzi Evidence Finder subito dopo averlo abilitato e il backfill di prove non è ancora completato, alcuni risultati potrebbero non essere disponibili. Per verificare lo stato del riempimento, vedereConferma dello stato di Evidence Finder .

La tua query di ricerca è riuscita

Gestione audit non può esportare i risultati di una query non riuscita. Per risolvere i problemi di una query non riuscita, consulta La mia query di ricerca non riesce.

Dopo aver confermato di soddisfare i prerequisiti, utilizza il seguente elenco di controllo per verificare la presenza di eventuali problemi:

1. Verifica lo stato della tua query di ricerca:
   a. La query è stata annullata? Evidence Finder mostra i risultati parziali elaborati prima dell'annullamento della query. Tuttavia, Gestione audit non esporta i risultati parziali nel bucket S3 o nel centro di download.
   b. La query è in esecuzione da più di un'ora? Le query che vengono eseguite per più di un'ora potrebbero scadere. Evidence Finder mostra i risultati parziali elaborati prima dello scadere del tempo a disposizione della query. Tuttavia, Gestione audit non esporta risultati parziali. Per evitare un timeout, puoi ridurre la quantità di prove da scansionare Modifica dei filtri di ricerca per specificare un intervallo di tempo più ristretto.
2. Controlla il nome e l'URI del bucket S3 di destinazione delle tue esportazioni:
   a. Il bucket specificato esiste? Se hai inserito manualmente l'URI di un bucket, assicurati di non aver commesso errori di digitazione. Un errore di battitura o un URI errato possono causare un errore `RESOURCE_NOT_FOUND` quando Gestione audit tenta di esportare il file CSV in Amazon S3.

3. Controlla le autorizzazioni del bucket S3 di destinazione delle tue esportazioni:

   a. Disponi delle autorizzazioni di scrittura per il bucket S3? Devi disporre dell'accesso in scrittura per il bucket S3 che stai utilizzando come destinazione di esportazione. Più specificamente, la policy di autorizzazione IAM deve includere un'`s3:PutObject`azione e l'ARN del bucket ed essere elencata CloudTrail come principale del servizio. Di seguito proponiamo un esempio di policy che puoi utilizzare.

4. Controlla se alcune delle tue Regione AWS informazioni non corrispondono:

   a. La Regione AWS chiave gestita dal cliente corrisponde Regione AWS alla tua valutazione? Se hai fornito una chiave gestita dal cliente per la crittografia dei dati, deve trovarsi nella stessa Regione AWS della tua valutazione. Per istruzioni su come modificare la chiave KMS, consultaConfigurazione delle impostazioni di crittografia dei dati.

5. Verifica le autorizzazioni del tuo account di amministratore delegato:

   a. La chiave gestita dal cliente nelle impostazioni di Gestione audit concede le autorizzazioni al tuo amministratore delegato? Se utilizzi un account di amministratore delegato e hai specificato una chiave gestita dal cliente per la crittografia dei dati, assicurati che l'amministratore delegato abbia accesso a quella chiave KMS. Per ulteriori informazioni, consulta Autorizzazione per gli utenti in altri account a utilizzare una chiave KMS nella Guida per gli sviluppatori AWS Key Management Service . Per rivedere e modificare le impostazioni di crittografia in Audit Manager, vedereConfigurazione delle impostazioni di crittografia dei dati.

> **Note**
>
> Quando modifichi le impostazioni di crittografia dei dati di Gestione audit, le modifiche si applicano alle nuove valutazioni che crei da quel momento in avanti. Ciò include tutti i file CSV esportati dalle nuove valutazioni.
> Le modifiche non si applicano alle valutazioni esistenti che hai creato prima di modificare le impostazioni di crittografia. Ciò include nuove esportazioni CSV create a partire da valutazioni esistenti, oltre alle esportazioni CSV esistenti. Le valutazioni esistenti, con tutte le relative esportazioni CSV, continuano a utilizzare la vecchia chiave KMS. Se l'identità IAM che esporta il file CVS non dispone delle autorizzazioni per utilizzare la vecchia chiave KMS, puoi concedere le autorizzazioni a livello di policy della chiave.

Non posso esportare prove specifiche dai miei risultati di ricerca

Tutti i risultati della tua ricerca sono inclusi nei risultati.

Se nel file CSV desideri includere solo prove specifiche, ti consigliamo di modificare i filtri di ricerca correnti. Questo ti permetterà di restringere i risultati in modo da individuare solo le prove che desideri esportare.

Non riesco a esportare più file CSV contemporaneamente

Questo errore è causato dall'esecuzione di troppe query CloudTrail Lake contemporaneamente.

Ciò può accadere se si raggruppano i risultati della ricerca e si tenta di esportare immediatamente un file CSV per ogni voce dei risultati raggruppati. Quando ottieni i risultati della ricerca ed esporti un file CSV, ognuna di queste azioni richiama una query. Puoi eseguire solo un massimo di cinque query per volta. Se stai eseguendo il numero massimo di query simultanee consentito, viene restituito un errore `MaxConcurrentQueriesException`.

Per evitare l'errore, assicurati di non esportare un numero eccessivo di file CSV contemporaneamente.

Per risolvere l'errore, attendi il completamento delle esportazioni CSV in corso. La maggior parte delle esportazioni richiede alcuni minuti. Tuttavia, se stai esportando una grande quantità di dati, il completamento dell'esportazione potrebbe richiedere fino a un'ora. Durante l'esportazione, puoi uscire da Evidence Finder.

Puoi controllare lo stato dell'esportazione dal centro di download, nella console di Gestione audit. Una volta completata l'esportazione dei file, torna ai risultati raggruppati in Evidence Finder. Potrai continuare a ottenere i risultati e a esportare un file CSV per ogni voce.

Risoluzione dei problemi relativi al framework

È possibile utilizzare le informazioni in questa pagina per risolvere problemi di framework comuni in Audit Manager.

Problemi generali relativi al framework

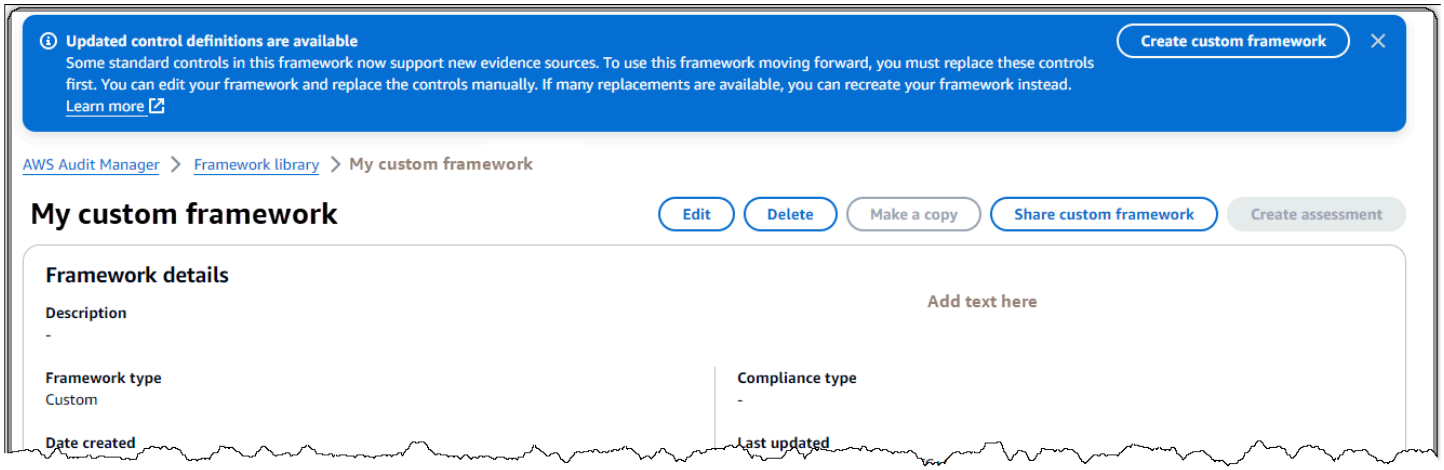
- Nella pagina dei dettagli del mio framework personalizzato, mi viene richiesto di ricreare il mio framework personalizzato

- Non riesco a creare una copia del mio framework personalizzato o utilizzarlo per creare una valutazione

Problemi di condivisione del framework

- Lo stato della richiesta di condivisione inviata viene visualizzato come Non riuscito
- La mia richiesta di condivisione è contrassegnata da un punto blu. Che cosa significa?
- Il mio framework condiviso dispone di controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?
- Ho aggiornato una regola personalizzata utilizzata in un framework condiviso. Devo fare qualcosa?

Nella pagina dei dettagli del mio framework personalizzato, mi viene richiesto di ricreare il mio framework personalizzato



Se viene visualizzato un messaggio che indica che sono disponibili definizioni di controllo aggiornate, significa che Audit Manager ora fornisce definizioni più recenti per alcuni dei controlli standard presenti nel framework personalizzato.

I controlli standard possono ora raccogliere prove daAWS managed source. Ciò significa che ogni volta che Audit Manager aggiorna le fonti di dati sottostanti per un controllo comune o di base, lo stesso aggiornamento viene applicato automaticamente ai controlli standard correlati. Ciò consente di garantire una conformità continua man mano che l'ambiente di conformità cloud cambia. Per assicurarti di trarre vantaggio da queste fonti AWS gestite, ti consigliamo di sostituire i controlli nel tuo framework personalizzato.

Nel framework personalizzato, Audit Manager indica per quali controlli sono disponibili sostitutivi. Dovrai sostituire questi controlli prima di poter creare una copia del tuo framework personalizzato o creare una valutazione da esso. La prossima volta che modificherai il tuo framework personalizzato, ti chiederemo di sostituire questi controlli insieme a qualsiasi altra modifica che desideri apportare.

Esistono due modi per sostituire i controlli nel framework personalizzato:

1. Ricrea il tuo framework personalizzato

Se è disponibile un numero elevato di controlli sostitutivi, ti consigliamo di ricreare il framework personalizzato. Questa è probabilmente l'opzione migliore se il framework personalizzato è basato su un framework standard.

- Ad esempio, supponiamo che tu abbia creato il tuo framework personalizzato utilizzando NIST SP 800-53 Rev. 5 come punto di partenza. Questo framework standard ha 1007 controlli standard e hai aggiunto 20 controlli personalizzati.
- In questo caso, l'opzione più efficiente è cercarla `NIST 800-53 (Rev. 5) Low-Moderate-High` nella libreria del framework e crearne una copia modificabile. Durante questo processo, puoi aggiungere gli stessi 20 controlli personalizzati utilizzati in precedenza. Poiché ora stai utilizzando l'ultima definizione del framework standard come punto di partenza, il framework personalizzato eredita automaticamente le definizioni più recenti per tutti i 1007 controlli standard.

2. Modifica il tuo framework personalizzato

Se sono disponibili delle sostituzioni per un numero limitato di controlli, ti consigliamo di modificare il framework personalizzato e sostituire i controlli manualmente.

- Ad esempio, supponiamo che tu abbia creato il tuo framework personalizzato da zero. Nel framework personalizzato, hai aggiunto 20 controlli personalizzati creati da te e otto controlli standard dal framework ACSC Essential Eight standard.
- In questo caso, poiché sarebbero disponibili aggiornamenti per un massimo di otto controlli, l'opzione più efficiente è modificare il framework personalizzato e sostituire tali controlli uno per uno. Per istruzioni, consultare la seguente procedura.

Per sostituire manualmente i controlli nel framework personalizzato

Per sostituire manualmente i controlli nel framework personalizzato

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Nel riquadro di navigazione a sinistra, scegli Libreria Framework, quindi scegli la scheda Framework personalizzati.
3. Seleziona il framework che si desideri modificare, scegli Azioni, quindi scegli Modifica.
4. Nella pagina Modifica dettagli del framework, scegli Avanti.
5. Nella pagina Modifica set di controlli, esamina il nome di ogni set di controlli per vedere se sono disponibili dei controlli sostitutivi.
6. Scegliete un set di controlli interessato per espanderlo e identificare quali dei relativi controlli devono essere sostituiti.

   > **Tip**
   >
   > Per identificare più rapidamente i controlli, inserisci **`Replacement available`** nella casella di ricerca.

7. Rimuovi i controlli interessati selezionando la casella di controllo e scegliendo Rimuovi dal set di controlli.
8. Aggiungi nuovamente gli stessi controlli. Questa azione sostituisce i controlli appena rimossi con la definizione di controllo più recente.

   a. In Aggiungi controlli, utilizza l'elenco a discesa Tipo di controllo e seleziona Controlli standard.

   b. Trova il sostituto del controllo che hai appena rimosso.

      > **Tip**
      >
      > In alcuni casi, il nome del controllo sostitutivo potrebbe non essere esattamente lo stesso dell'originale. In questo caso, è probabile che il nome del controllo sostitutivo sia molto simile all'originale. In rari casi, un controllo può essere sostituito da due controlli (o viceversa).
      > Se non riesci a trovare un controllo sostitutivo, ti consigliamo di eseguire una ricerca parziale. A tale scopo, inserisci parte del nome del controllo originale o una

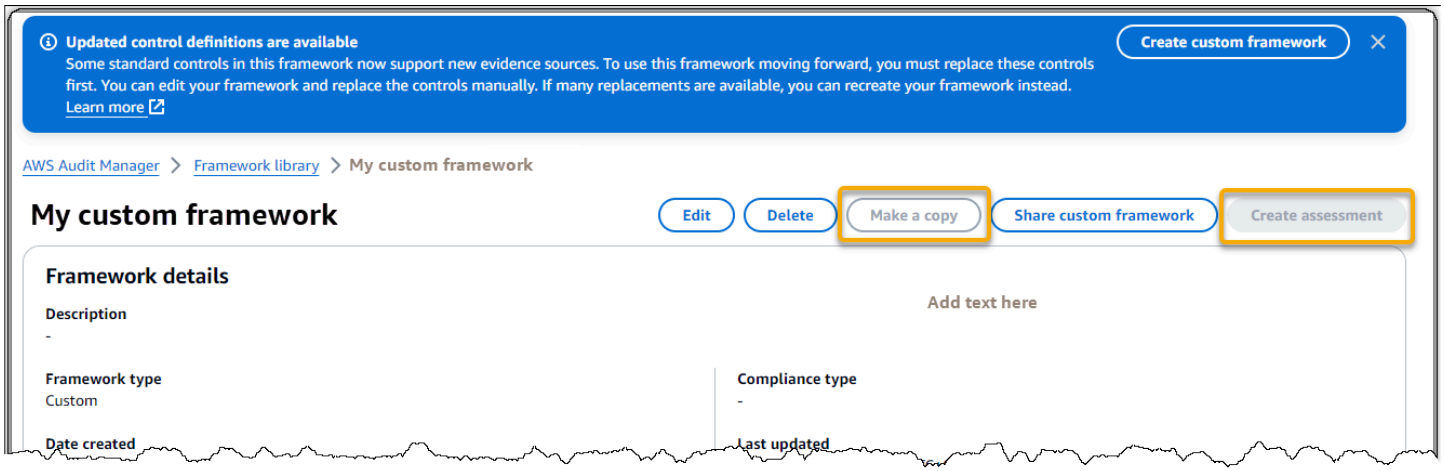
parola chiave che rappresenti ciò che stai cercando. Puoi anche cercare per tipo di conformità per restringere ulteriormente l'elenco dei risultati.

c. Seleziona la casella di controllo accanto a un controllo e scegli Aggiungi al set di controlli.

d. Nella finestra pop-up che appare, scegli Aggiungi per confermare.

9. Ripeti i passaggi 6-8 secondo necessità fino a sostituire tutti i controlli.
10. Seleziona Successivo.
11. Nella pagina Rivedi e salva, scegli Salva modifiche.

Non riesco a creare una copia del mio framework personalizzato o utilizzarlo per creare una valutazione



Se i pulsanti Crea una copia e Crea valutazione non sono disponibili nella pagina dei dettagli del framework, significa che devi sostituire alcuni controlli nel framework personalizzato.

Per istruzioni su come procedere, consultaNella pagina dei dettagli del mio framework personalizzato, mi viene richiesto di ricreare il mio framework personalizzato.

Lo stato della richiesta di condivisione inviata viene visualizzato come Non riuscito

Se provi a condividere un framework personalizzato e l'operazione non riesce, ti consigliamo di controllare quanto segue:

1. Assicurati che Audit Manager sia abilitato nella regione del destinatario Account AWS e nella regione specificata. Per un elenco delle AWS Audit Manager regioni supportate, consulta AWS Audit Manager endpoint e quote nell'Amazon Web Services General Reference.
2. Assicurati di aver inserito l' Account AWS ID corretto quando hai specificato l'account del destinatario.
3. Assicurati di non aver specificato un account di AWS Organizations gestione come destinatario. Puoi condividere un framework personalizzato con un amministratore delegato, ma se tenti di condividere un framework personalizzato con un account di gestione, l'operazione non riesce.
4. Se utilizzi una chiave gestita dal cliente per crittografare i tuoi dati di Gestione audit, assicurati che la chiave KMS sia abilitata. Se la tua chiave KMS è disabilitata e provi a condividere un framework personalizzato, l'operazione avrà esito negativo. Per istruzioni su come abilitare una chiave KMS disabilitata, consulta Abilitazione e disabilitazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service

La mia richiesta di condivisione è contrassegnata da un punto blu. Che cosa significa?

Una notifica con il punto blu indica che una richiesta di condivisione richiede la tua attenzione.

Notifica con il punto blu per i mittenti

Una notifica con il punto blu appare accanto alle richieste di condivisione inviate con uno stato di In scadenza. Gestione audit visualizza la notifica con il punto blu in modo che tu possa ricordare al destinatario di agire sulla richiesta di condivisione prima che scada.

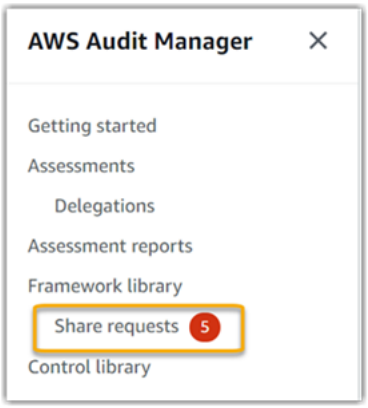
Affinché la notifica con il punto blu scompaia, il destinatario deve accettare o rifiutare la richiesta. Il punto blu scompare anche se revochi la richiesta di condivisione.

Puoi utilizzare la procedura seguente per verificare la presenza di eventuali richieste di condivisione in scadenza e inviare un promemoria facoltativo al destinatario affinché intervenga.

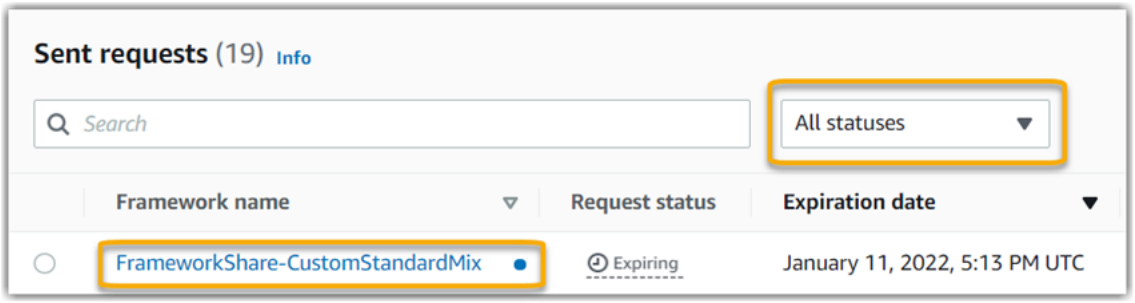
Per visualizzare le notifiche relative alle richieste inviate

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Se hai una notifica di richiesta di condivisione, Gestione audit visualizza un punto rosso accanto all'icona del menu di navigazione.

3. Espandi il riquadro di navigazione e guarda accanto a Condividi richieste. Un badge di notifica indica il numero di richieste di condivisione che necessitano attenzione.



4. Scegli Richieste di condivisione, quindi scegli la scheda Richieste inviate.
5. Cerca il punto blu per identificare le richieste di condivisione in scadenza entro i prossimi 30 giorni. In alternativa, puoi anche visualizzare le richieste di condivisione in scadenza selezionando In scadenza dal menu a discesa del filtro Tutti gli stati.



6. (Facoltativo) Ricorda al destinatario che deve agire sulla richiesta di condivisione prima che scada. Questo passaggio è facoltativo, poiché Gestione audit invia una notifica nella console per informare il destinatario quando una richiesta di condivisione è attiva o in scadenza. Tuttavia, anche tu puoi inviare un promemoria al destinatario utilizzando il tuo canale di comunicazione preferito.

Notifiche con punti blu per i destinatari

Una notifica con il punto blu appare accanto alle richieste di condivisione ricevute il cui stato sia Attivo o In scadenza. Gestione audit visualizza la notifica con il punto blu per ricordarti di agire sulla richiesta di condivisione prima che scada. Affinché la notifica con il punto blu scompaia, devi

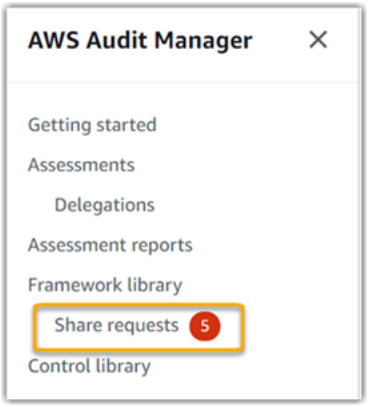
accettare o rifiutare la richiesta. Il punto blu scompare anche se il mittente revoca la richiesta di condivisione.

Per verificare la presenza di richieste di condivisione attive e in scadenza, utilizza la procedura indicata di seguito.

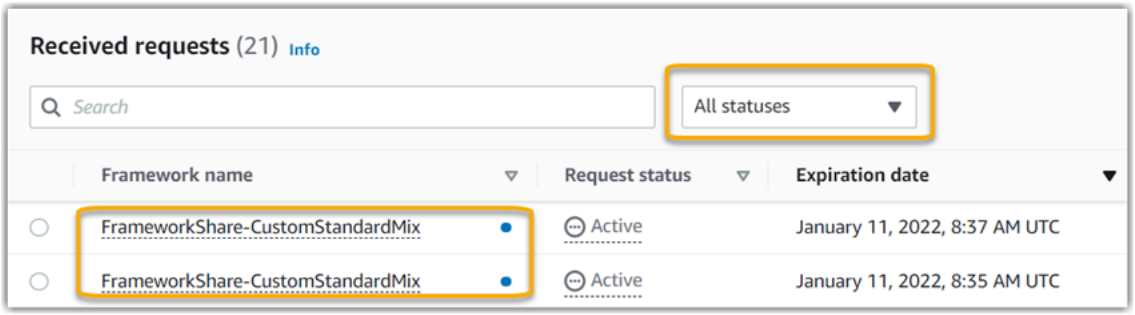
Per visualizzare le notifiche relative alle richieste ricevute

1. Apri la console di Gestione audit AWS all'indirizzo https://console.aws.amazon.com/auditmanager/home.
2. Se hai una notifica di richiesta di condivisione, Gestione audit visualizza un punto rosso accanto all'icona del menu di navigazione.

3. Espandi il riquadro di navigazione e guarda accanto a Condividi richieste. Un badge di notifica indica il numero di richieste di condivisione che necessitano della tua attenzione.



4. Scegli Richieste di condivisione. Per impostazione predefinita, questa pagina si apre sulla scheda Richieste ricevute.
5. Identifica le richieste di condivisione che richiedono il tuo intervento cercando gli elementi con un punto blu.



6. (Facoltativo) Per visualizzare solo le richieste in scadenza nei prossimi 30 giorni, trova l'elenco a discesa Tutti gli stati e seleziona In scadenza.

Il mio framework condiviso dispone di controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?

Sì, il tuo destinatario può raccogliere prove per questi controlli, ma a tal fine sono necessari alcuni passaggi.

Affinché Audit Manager raccolga prove utilizzando una AWS Config regola come mappatura dell'origine dati, deve essere vero quanto segue. Questi criteri si applicano sia alle regole gestite sia alle regole personalizzate.

- La regola deve esistere nell' AWS ambiente del destinatario.
- La regola deve essere abilitata nell' AWS ambiente del destinatario.

Ricorda che le AWS Config regole del tuo account probabilmente non esistono già nell' AWS ambiente del destinatario. Inoltre, quando il destinatario accetta la richiesta di condivisione, Gestione audit non ricrea nessuna delle tue regole personalizzate nel suo account. Affinché il destinatario possa raccogliere prove utilizzando le tue regole personalizzate come mappatura dell'origine dati, deve creare le stesse regole personalizzate nella sua istanza di AWS Config. Dopo che il destinatario ha creato e quindi abilitato le regole AWS Config, Audit Manager può raccogliere prove da tale fonte di dati.

Ti consigliamo di comunicare con il destinatario per fargli sapere se è necessario creare AWS Config regole personalizzate per la sua istanza di AWS Config.

Ho aggiornato una regola personalizzata utilizzata in un framework condiviso. Devo fare qualcosa?

Per gli aggiornamenti delle regole all'interno del tuo AWS ambiente

Quando si aggiorna una regola personalizzata all'interno del proprio AWS ambiente, non è necessaria alcuna azione in Audit Manager. Gestione audit rileva e gestisce gli aggiornamenti delle regole come descritto nella tabella seguente. Gestione audit non invia notifiche quando rileva un aggiornamento delle regole.

Scenario	Cosa fa Gestione audit	Cosa devi fare tu
Una regola personalizzata viene aggiornata nell'istanza di AWS Config.	Gestione audit continua a segnalare gli esiti di quella regola utilizzando la definizione di regola aggiornata.	Non è richiesta alcuna azione.
Una regola personalizzata viene eliminata nell'istanza di AWS Config.	Gestione audit interrompe la segnalazione degli esiti della regola eliminata.	Non è richiesta alcuna azione. Se lo desideri, puoi modificare i controlli personalizzati che utilizzavano la regola eliminata come mappatura dell'origine dati. Puoi quindi rimuovere la regola eliminata per ripulire le impostazioni dell'origine dati del controllo. In caso contrario, il nome della regola eliminata rimane come una mappatura dell'origine dati inutilizzata.

Per gli aggiornamenti delle regole al di fuori AWS dell'ambiente

Nell' AWS ambiente del destinatario, Audit Manager non rileva l'aggiornamento delle regole. Questo perché mittenti e destinatari lavorano ciascuno in ambienti separati AWS . La tabella seguente indica le azioni consigliate per questo scenario.

Il tuo ruolo	Scenario	Azione consigliata
Mittent	• Hai condiviso un framework che utilizza regole personalizzate come mappatura dell'origine dati. • Dopo aver condiviso il framework, hai aggiornato o eliminato una di queste regole in. AWS Config	Contatta il destinatario per informarlo dell'aggiornamento. In questo modo, potrà effettuare lo stesso aggiornamento e rimanere sincronizzato con l'ultima definizione della regola.

Il tuo ruolo	Scenario	Azione consigliata
Destinatario	• Hai accettato un framework condiviso che utilizza regole personalizzate come mappatura dell'origine dati. • Dopo aver ricreato le regole personalizzate nell'istanza di AWS Config, il mittente ha aggiornato o eliminato una di tali regole.	Aggiorna la regola corrispondente nella tua istanza di AWS Config.

Risoluzione dei problemi di notifica

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti le notifiche in Gestione audit.

Argomenti

- Ho specificato un argomento di Amazon SNS in Gestione audit, ma non ho ricevuto alcuna notifica
- Ho specificato un argomento FIFO, ma non ricevo notifiche nell'ordine previsto

Ho specificato un argomento di Amazon SNS in Gestione audit, ma non ho ricevuto alcuna notifica

Se il tuo argomento su Amazon SNS utilizza AWS KMS la crittografia lato server (SSE), potresti non avere le autorizzazioni necessarie per la tua policy chiave. AWS KMS Potresti anche non ricevere le notifiche se non hai sottoscritto un endpoint per il tuo argomento.

Se non ricevi notifiche, assicurati di avere eseguito le seguenti operazioni:

- Hai allegato la policy di autorizzazioni richiesta alla tua chiave KMS. Per un esempio di politica che puoi utilizzare, consulta. Esempio 2 (Autorizzazioni per la chiave KMS allegata all'argomento SNS)
- Hai sottoscritto un endpoint per l'argomento tramite il quale vengono inviate le notifiche. Quando effettui la sottoscrizione di un endpoint e-mail a un argomento, ricevi un'e-mail con la conferma di sottoscrizione. Devi confermare la sottoscrizione per iniziare a ricevere le notifiche e-mail. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon SNS.

Ho specificato un argomento FIFO, ma non ricevo notifiche nell'ordine previsto

Gestione audit supporta l'invio di notifiche agli argomenti FIFO SNS. Tuttavia, l'ordine in cui Gestione audit invia le notifiche agli argomenti FIFO non è garantito.

Risoluzione dei problemi di autorizzazione e accesso

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti le autorizzazioni in Gestione audit.

Argomenti

Ho seguito la procedura di configurazione di Gestione audit, ma non dispongo di privilegi IAM sufficienti

L'utente, il ruolo o il gruppo utilizzato per accedere a Gestione audit deve disporre delle autorizzazioni necessarie. Inoltre, la tua policy basata sull'identità non dovrebbe essere troppo restrittiva. In caso contrario, la console non funzionerà come previsto. Questa guida fornisce un esempio di politica che puoi utilizzare perConsenti le autorizzazioni minime richieste per abilitare Gestione audit. A seconda del caso d'uso, potresti aver bisogno di autorizzazioni più ampie e meno restrittive. Ad esempio, consigliamo che i proprietari dell'audit abbiano l'accesso come amministratore. In questo modo possono modificare le impostazioni di Gestione audit e gestire risorse come valutazioni, framework, controlli e report di valutazione. Altri utenti, come i delegati, potrebbero aver bisogno solo dell'accesso di gestione o di sola lettura.

Assicurati di aggiungere le autorizzazioni appropriate per il tuo utente, ruolo o gruppo. Per i titolari degli audit, la politica consigliata è AWSAuditManagerAdministratorAccess. Per i delegati, puoi utilizzare la policy di esempio di accesso alla gestione fornita nella pagina degli esempi di policy IAM. Puoi utilizzare queste policy di esempio come punto di partenza e apportare le modifiche necessarie per soddisfare le tue esigenze.

Ti consigliamo di dedicare del tempo alla personalizzazione delle autorizzazioni in modo che soddisfino le tue esigenze specifiche. Per ulteriore assistenza con le autorizzazioni IAM, contatta l'amministratore o il Supporto AWS.

Ho indicato qualcuno come proprietario dell'audit, ma non ha ancora pieno accesso alla valutazione. Perché?

Specificare qualcuno solamente come proprietario dell'audit non significa che abbia pieno accesso a una valutazione. I proprietari degli audit devono inoltre disporre delle autorizzazioni IAM necessarie per accedere e gestire le risorse di Gestione audit. In altre parole, oltre a specificare un utente come proprietario dell'audit, devi anche allegare le policy IAM necessarie a quell'utente. L'idea alla base di ciò è che, richiedendo entrambi, Gestione audit garantisca il pieno controllo su tutte le specifiche di ciascuna valutazione.

> **Note**
>
> Per i titolari di audit, consigliamo di utilizzare la AWSAuditManagerAdministratorAccesspolicy. Per ulteriori informazioni, consulta Politiche consigliate per gli utenti in AWS Audit Manager.

Non riesco a eseguire un'operazione in Gestione audit

Se non disponi delle autorizzazioni necessarie per utilizzare la AWS Audit Manager console o le operazioni dell'API Audit Manager, è probabile che si verifichi un `AccessDeniedException` errore.

Per risolvere il problema, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse di Audit Manager

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Gestione audit supporta queste funzionalità, consulta Come AWS Audit Manager funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Vedo un errore di accesso negato, nonostante disponga delle autorizzazioni di Audit Manager richieste

Se il tuo account fa parte di un'organizzazione, è possibile che l'`Access Denied`errore sia causato da una policy di controllo dei servizi (SPC). Gli SCP sono policy utilizzate per gestire le autorizzazioni di un'organizzazione. Quando un SCP è attivo, può negare autorizzazioni specifiche a tutti gli account dei membri, incluso l'account amministratore delegato utilizzato in Audit Manager.

Ad esempio, se l'organizzazione dispone di un SCP che nega le autorizzazioni per le API di AWS Control Catalog, non è possibile visualizzare le risorse fornite da Control Catalog. Questo vale anche se altrimenti disponi delle autorizzazioni necessarie per Audit Manager, come la AWSAuditManagerAdministratorAccesspolicy. L'SCP sovrascrive le autorizzazioni delle policy gestite negando esplicitamente l'accesso alle API del Control Catalog.

Ecco un esempio di tale SCP. Con questo SCP in atto, all'account amministratore delegato viene negato l'accesso ai controlli, agli obiettivi di controllo e ai domini di controllo comuni necessari per utilizzare la funzionalità di controlli comuni in Audit Manager.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains",
            ],
            "Resource": "*"
        }
    ]
}
```

Per risolvere questo problema, ti consigliamo di eseguire le seguenti operazioni:

1. Conferma se un SCP è collegato alla tua organizzazione. Per istruzioni, consulta Ottenere informazioni sulle policy della tua organizzazione nella AWS Organizations User Guide.
2. Identifica se l'`Access Denied`errore è causato da SCP.
3. Aggiorna SCP per assicurarti che il tuo account amministratore delegato disponga dell'accesso necessario per Audit Manager. Per istruzioni, consulta Updating an SCP nella AWS Organizations User Guide.

Risorse aggiuntive

Le pagine seguenti contengono indicazioni per la risoluzione di altri problemi che possono essere causati dalla mancanza di autorizzazioni:

- Non riesco a vedere alcun controllo o set di controlli nella mia valutazione
- L'opzione delle regole personalizzate non è disponibile quando configuro un'origine dati di controllo
- Ricevo un errore di accesso negato quando provo a generare un report
- Ricevo un errore di accesso negato quando provo a generare un report di valutazione utilizzando il mio account di amministratore delegato
- Non riesco ad abilitare Evidence Finder
- Non riesco a disabilitare Evidence Finder
- La mia query di ricerca non riesce
- Ho specificato un argomento di Amazon SNS in Gestione audit, ma non ho ricevuto alcuna notifica

Taggare le risorse AWS Audit Manager

Un tag è un'etichetta di metadati che si assegna o che si assegna a AWS una risorsa. AWS Ciascun tag è formato da una chiave e da un valore, Per i tag assegnati da te, puoi definire la chiave e il valore. Ad esempio, potresti definire la chiave come `stagee` il valore di una risorsa come `test`.

I tag consentono di:

- Individua facilmente le tue risorse Gestione audit. È possibile utilizzare i tag come criteri di ricerca quando si naviga nella libreria del framework e nella libreria di controllo.
- Associa la tua risorsa a un tipo di conformità. Puoi etichettare più risorse con un tag specifico per la conformità per associare tali risorse a un framework specifico.
- Identifica e organizza le tue risorse. AWS Molti Servizi AWS supportano l'etichettatura, quindi puoi assegnare lo stesso tag a risorse di servizi diversi per indicare che le risorse sono correlate.
- Tieni traccia dei costi. AWS Attivi questi tag sulla AWS Billing and Cost Management dashboard. AWS utilizza i tag per classificare i costi e fornirti un rapporto mensile sull'allocazione dei costi. Per ulteriori informazioni, consulta la pagina sull'utilizzo dei tag per l'allocazione dei costi nella AWS Billing and Cost Management Guida per l'utente.

Le seguenti sezioni forniscono ulteriori informazioni sui tag per. AWS Audit Manager

Indice

Risorse supportate in Gestione audit

Le seguenti risorse di Gestione audit supportano l'assegnazione dei tag:

- Valutazioni
- Controlli
- Framework

Limitazioni applicate ai tag

Le seguenti restrizioni di base si applicano ai tag sulle risorse di Gestione audit:

- Numero massimo di tag che è possibile assegnare a una risorsa: 50
- Lunghezza massima della chiave: 128 caratteri Unicode
- Lunghezza massima del valore: 256 caratteri Unicode
- Caratteri validi per chiave e valore: a-z, A-Z, 0-9, spazi e i seguenti caratteri: _ . : / = + - e @
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole
- Non utilizzare `aws:` come prefisso per le chiavi; è riservato all'uso AWS

Risorse aggiuntive

È possibile impostare i tag come proprietà quando si crea una valutazione, un framework o un controllo. È possibile aggiungere, modificare ed eliminare tag tramite la console Audit Manager, AWS Command Line Interface (AWS CLI) e l'API Audit Manager. Per ulteriori informazioni, consulta i collegamenti seguenti:

- Per etichettare le valutazioni:
  - Creazione di una valutazione in AWS Audit Manager e Modificare una valutazione in AWS Audit Manager nella sezione Valutazioni di questa guida
  - Scheda Tagnella pagina Rivedi una valutazione di questa guida
  - CreateAssessmente UpdateAssessmentnell'AWS Audit Manager API Reference
  - TagResourcee UntagResourcenell'AWS Audit Manager API Reference
- Per i framework di etichettatura:
  - Creazione di un framework personalizzato in AWS Audit Manager e Modifica di un framework personalizzato in AWS Audit Manager nella sezione relativa alla libreria Framework di questa guida
  - Nella Tags tab pagina Visualizza i dettagli del framework di questa guida
  - CreateAssessmentFrameworke UpdateAssessmentFrameworknell'AWS Audit Manager API Reference
  - TagResourcee UntagResourcenell'AWS Audit Manager API Reference
- Per i controlli di etichettatura:

- Creazione di un controllo personalizzato in AWS Audit Manager e Modifica di un controllo personalizzato in AWS Audit Manager nella sezione Libreria di controlli di questa guida
- La Tags sezione della pagina Revisione di un controllo personalizzato di questa guida
- La Tags sezione sulla pagina Revisione di una pagina di controllo standard di questa guida
- CreateControle UpdateControlnell'AWS Audit Manager API Reference
- TagResourcee UntagResourcenell'AWS Audit Manager API Reference

Comprensione delle quote e delle restrizioni per AWS Audit Manager

Your Account AWS ha delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, per altre non è possibile.

La maggior parte delle quote di Audit Manager, ma non tutte, sono elencate nel AWS Audit Manager namespace nella console Service Quotas. Per sapere come richiedere un aumento delle quote, consulta Gestione delle proprie quote di Gestione audit.

Indice

Quote predefinite di Gestione audit

Le seguenti AWS Audit Manager quote si riferiscono a ciascuna regione. Account AWS

Risorsa	Quota
Valutazioni	Numero di valutazioni attive per account: 100
Rapporti di valutazione	Numero di elementi di prova che puoi aggiungere a un report di valutazione: • Per i report della stessa regione (in cui la valutazione e il bucket S3 di destinazione del report di valutazione si trovano nella stessa Regione AWS): 22.000 • Per i report interregionali (in cui la valutazione e il bucket S3 di destinazione del report di valutazione si trovano in Regioni AWS differenti): 3.500 • Per i report in cui la relativa valutazione utilizza un servizio gestito dal cliente AWS KMS key: 3.500

Risorsa	Quota
Controlli	Numero di controlli personalizzati per account: 500
Evidenza	Dimensione massima di un singolo file di prove manuali: 100 MB Numero giornaliero di caricamenti di prove manuali per controllo: 100 **Tip** Per caricare una grande quantità di prove manuali su un unico controllo, consigliamo di caricarle in batch nell'arco di diversi giorni.
Framework	Numero di framework personalizzati per account: 100 **Note** Le quote di framework si applicano a tutti i framework personalizzati condivisi presenti nella tua libreria di framework, indipendentemente da chi li ha creati.
Destinatari del framework personalizzato condiviso	Numero di account di destinatari attivi: 100
Accesso all'API	Numero di transazioni al secondo (TPS) su tutte le API: 20 TPS

Gestione delle proprie quote di Gestione audit

AWS Audit Manager è integrato con Service Quotas e consente di visualizzare e gestire le quote da una posizione centrale. Servizio AWS Service Quotas semplifica la ricerca del valore di tutte le proprie quote di Gestione audit.

Per visualizzare le Service Quotas di Gestione audit utilizzando la console

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/.

2. Nel riquadro di navigazione, scegli Servizi AWS.
3. Nell’elenco Servizi AWS, cerca e seleziona AWS Audit Manager.
4. Nell'elenco delle quote di servizio, è possibile visualizzare il nome della quota di servizio, il valore della quota applicata (se disponibile), il valore della quota AWS predefinita e se la quota è regolabile.
5. Per visualizzare ulteriori informazioni su una quota di servizio, ad esempio la descrizione, scegli il nome della quota.
6. (Facoltativo) Per richiedere un aumento della quota, seleziona la quota che desideri aumentare, seleziona Richiedi un aumento della quota, inserisci o seleziona le informazioni richieste e seleziona Richiedi.

Risorse aggiuntive

Per ulteriori informazioni su come gestire le quote, consulta Richiedere un aumento delle quote nella Service Quotas User Guide.

Per ulteriori informazioni sulle quote di servizio, consulta la sezione che descrive cosa solo le quote di servizio nella Guida per l'utente delle quote di servizio.

Comprendere la sicurezza e la protezione dei dati in AWS Audit Manager

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che funziona Servizi AWS nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS Audit Manager, consulta AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dall'uso Servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Audit Manager. I seguenti argomenti illustrano come configurare Gestione audit per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere le tue risorse di Audit Manager.

Argomenti

Protezione dei dati in AWS Audit Manager

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Audit Manager. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Audit Manager o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Oltre al suggerimento di cui sopra, consigliamo in particolare ai clienti di Gestione audit di non includere informazioni sensibili di identificazione nei campi liberi durante la creazione di valutazioni, controlli personalizzati, framework personalizzati e commenti di delega.

Eliminazione dei dati di Gestione audit

Esistono vari modi per eliminare i dati Gestione audit.

Eliminazione dei dati quando si disabilita Gestione audit

Quando disabiliti Gestione audit, puoi decidere se eliminare tutti i tuoi dati di Gestione audit. Se scegli di eliminare i tuoi dati, questi verranno eliminati entro 7 giorni dalla disattivazione di Gestione audit. Dopo aver eliminato i tuoi dati, non puoi recuperarli.

Eliminazione automatica dei dati

Alcuni dati di Gestione audit vengono eliminati automaticamente dopo un determinato periodo di tempo. Gestione audit conserva i dati dei clienti come segue.

Tipo di dati	Periodo di conservazione dei dati	Note
Prove	I dati vengono conservati per 2 anni dal momento della creazione	Include prove automatiche e prove manuali
Risorse create dai clienti	I dati vengono conservati a tempo indeterminato	Include valutazioni, report di valutazione, controlli personalizzati e framework personalizzati

Eliminazione manuale dei dati

Puoi eliminare singole risorse Gestione audit in qualsiasi momento. Per le istruzioni, consulta quanto segue:

- Eliminazione di una valutazione in AWS Audit Manager

  - Vedi anche: DeleteAssessmentnell'AWS Audit Manager API Reference
- Eliminazione di un framework personalizzato in AWS Audit Manager
  - Vedi anche: DeleteAssessmentFrameworknell'AWS Audit Manager API Reference
- Eliminazione delle richieste di condivisione in AWS Audit Manager
  - Vedi anche: DeleteAssessmentFrameworkSharenell'AWS Audit Manager API Reference
- Eliminazione di un report di valutazioni
  - Vedi anche: DeleteAssessmentReportnell'AWS Audit Manager API Reference
- Eliminazione di un controllo personalizzato in AWS Audit Manager
  - Vedi anche: DeleteControlnell'AWS Audit Manager API Reference

Per eliminare altri dati di risorse che potresti aver creato durante l'utilizzo di Gestione audit, consulta quanto segue:

- Eliminare un archivio dati di eventi nella AWS CloudTrail Guida per l'utente
- Cos'è un bucket nella Guida per l'utente di Amazon Simple Storage Service (Amazon S3)

Crittografia a riposo

Per crittografare i dati inattivi, Audit Manager utilizza la crittografia lato server Chiavi gestite da AWS per tutti i suoi archivi di dati e registri.

I dati vengono crittografati con una chiave gestita dal cliente o Chiave di proprietà di AWS, a seconda delle impostazioni selezionate. Se non fornisci una chiave gestita dal cliente, Audit Manager utilizza an Chiave di proprietà di AWS per crittografare i tuoi contenuti. Tutti i metadati di servizio in DynamoDB e Amazon S3 in Gestione audit sono crittografati utilizzando una Chiave di proprietà di AWS.

Gestione audit crittografa i dati come segue:

- I metadati di servizio archiviati in Amazon S3 sono crittografati con Chiave di proprietà di AWS SSE-KMS.
- I metadati di servizio archiviati in DynamoDB sono crittografati lato server utilizzando KMS e una Chiave di proprietà di AWS.
- I contenuti archiviati in DynamoDB sono crittografati lato client utilizzando una chiave gestita dal cliente o una Chiave di proprietà di AWS. La chiave KMS si basa sulle impostazioni scelte.

- I tuoi contenuti archiviati in Amazon S3 in Gestione audit sono crittografati tramite SSE-KMS. La chiave KMS si basa sulla selezione effettuata e può essere una chiave gestita dal cliente o una Chiave di proprietà di AWS.
- I report di valutazione pubblicati nel tuo bucket S3 sono crittografati come segue:
  - Se hai fornito una chiave gestita dal cliente, i tuoi dati vengono crittografati utilizzando SSE-KMS.
  - Se hai utilizzato il Chiave di proprietà di AWS, i tuoi dati vengono crittografati utilizzando SSE-S3.

Crittografia in transito

Gestione audit fornisce endpoint sicuri e privati per la crittografia dei dati in transito. Gli endpoint sicuri e privati consentono di AWS proteggere l'integrità delle richieste API all'Audit Manager.

Transito tra servizi

Per impostazione predefinita, tutte le comunicazioni tra servizi sono protette tramite crittografia Transport Layer Security (TLS).

Gestione delle chiavi

Audit Manager supporta Chiavi di proprietà di AWS sia chiavi gestite dal cliente sia chiavi gestite dal cliente per la crittografia di tutte le risorse di Audit Manager (valutazioni, controlli, framework, prove e report di valutazione salvati nei bucket S3 nei tuoi account).

Ti consigliamo di utilizzare una chiave gestita dal cliente. In questo modo, puoi visualizzare e gestire le chiavi di crittografia che proteggono i tuoi dati, inclusa la visualizzazione dei log del loro utilizzo in AWS CloudTrail. Quando scegli una chiave gestita dal cliente, Gestione audit crea una concessione sulla chiave KMS in modo che possa essere utilizzata per crittografare i contenuti.

> **Warning**
>
> Dopo l'eliminazione o la disattivazione di una chiave KMS utilizzata per crittografare le risorse Gestione audit, non è più possibile decrittare le risorse crittografate usando tale chiave KMS, che quindi non possono più essere recuperate.
> L'eliminazione di una chiave KMS in () è distruttiva e potenzialmente pericolosa AWS Key Management Service .AWS KMS Per ulteriori informazioni sull'eliminazione delle chiavi KMS, consulta Eliminazione AWS KMS keys nella AWS Key Management Service Guida per l'utente.

È possibile specificare le impostazioni di crittografia quando si abilita Audit Manager utilizzando l' AWS Management Console API Audit Manager o AWS Command Line Interface (AWS CLI). Per istruzioni, consulta Abilitazione AWS Audit Manager.

Puoi rivedere e modificare le tue impostazioni di crittografia in qualsiasi momento. Per istruzioni, consulta Configurazione delle impostazioni di crittografia dei dati.

Per ulteriori informazioni su come configurare le chiavi gestite dal cliente, consulta Creazione di chiavi nella AWS Key Management Service Guida per l'utente.

Gestione delle identità e degli accessi per AWS Audit Manager

AWS Identity and Access Management (IAM) aiuta un Servizio AWS amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse Gestione audit. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Audit Manager.

Utente del servizio: se utilizzi il servizio Gestione audit per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità

Gestione audit utilizzate per il lavoro potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Gestione audit, consulta Risoluzione dei problemi relativi all' AWS Audit Manager identità e all'accesso.

Amministratore del servizio: se sei il responsabile delle risorse Gestione audit presso la tua azienda, probabilmente disponi dell'accesso completo a Gestione audit. Il tuo compito è determinare le funzionalità e le risorse Gestione audit a cui gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Gestione audit consulta Come AWS Audit Manager funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a Gestione audit. Per visualizzare policy basate su identità Gestione audit di esempio che possono essere utilizzate in IAM, consulta Esempi di policy basate sull'identità per AWS Audit Manager.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del

metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web AWS Directory Service, la directory Identity Center o qualsiasi utente che accede Servizi AWS utilizzando credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali

temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni,

crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi

limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Audit Manager funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Gestione audit, scopri quali funzionalità di IAM sono disponibili per l'uso con Gestione audit.

Funzionalità IAM che puoi utilizzare con AWS Audit Manager

Funzionalità IAM	Supporto Gestione audit
Policy basate su identità	Sì

Funzionalità IAM	Supporto Gestione audit
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Parziale
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come AWS Audit Manager e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS Audit Manager

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica

all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

AWS Audit Manager crea una policy gestita denominata `AWSAuditManagerAdministratorAccess` per gli amministratori di Audit Manager. Questa policy garantisce l'accesso amministrativo completo in Gestione audit. Gli amministratori possono associare questa policy a qualsiasi ruolo o utente esistente o creare un nuovo ruolo con questa policy.

Politiche consigliate per gli utenti in AWS Audit Manager

AWS Audit Manager consente di mantenere la separazione delle mansioni tra i diversi utenti e per diversi audit utilizzando diverse policy IAM. Le due persone in Gestione audit e le relative politiche consigliate sono definite come segue.

Utente	Descrizione e politicy consigliata
Proprietario dell'audit	• Questa persona deve disporre delle autorizzazioni necessarie per gestire le valutazioni in. AWS Audit Manager • La politica consigliata da utilizzare per questa persona è la politica gestita denominata. AWSAuditManagerAdministratorAccess È possibile utilizzare questa policy come punto di partenza e definire le autorizzazioni in base alle esigenze.
Delegato	• Questa persona può accedere ai set di controlli delegati in una valutazione. Può aggiornare lo stato del controllo, aggiungere commenti, inviare un set di controlli per la revisione e aggiungere prove al rapporto di valutazione. • La policy consigliata da utilizzare per questa persona è la seguente policy di esempio: Consentire l'accesso alla gestione degli utenti a AWS Audit Manager. Puoi utilizzare questa policy come punto di partenza e apportare le modifiche necessarie per soddisfare le tue esigenze.

Esempi di policy basate sull'identità per AWS Audit Manager

Per visualizzare esempi di policy basate su identità Gestione audit, consulta Esempi di policy basate sull'identità per AWS Audit Manager.

Politiche basate sulle risorse all'interno AWS Audit Manager

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per AWS Audit Manager

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Audit Manager azioni, consulta Azioni definite da AWS Audit Manager nel Service Authorization Reference.

Le azioni politiche in AWS Audit Manager uso utilizzano il seguente prefisso prima dell'azione.

```
auditmanager
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Get`, includi la seguente operazione.

```
"Action": "auditmanager:Get*"
```

Per visualizzare esempi di policy basate su identità Gestione audit, consulta Esempi di policy basate sull'identità per AWS Audit Manager.

Risorse politiche per AWS Audit Manager

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di AWS Audit Manager risorse e dei relativi ARN, consulta Resources defined by AWS Audit Manager nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da Gestione audit AWS.

Una valutazione Gestione audit presenta il seguente formato nome della risorsa Amazon (ARN):

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Un set di controlli Gestione audit presenta il seguente formato ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Un controllo Gestione audit presenta il seguente formato ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Name (ARN).

Ad esempio, per specificare la valutazione `i-1234567890abcdef0` nell'istruzione, utilizza il seguente ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Per specificare tutte le istanze database che appartengono a un account specifico, utilizza il carattere jolly (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Alcune operazioni Gestione audit, ad esempio quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Molte operazioni API di Gestione audit coinvolgono più risorse. Ad esempio, `ListAssessments` restituisce un elenco di metadati di valutazione accessibili dalle persone attualmente connesse. Account AWS Pertanto, un utente deve disporre delle autorizzazioni per visualizzare le valutazioni. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
      "resource2"
```

Per un elenco di tipi di risorse di Gestione audit e i relativi ARN, consulta Risorse definite da AWS Audit Managernella Guida per l'utente IAM. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS Audit Manager.

Alcune operazioni API di Gestione audit supportano più risorse. Ad esempio, `GetChangeLogs` accede a una `assessmentID`, `controlID` e `controlSetId`, quindi un principale deve disporre delle autorizzazioni per accedere a ciascuna di queste risorse. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Chiavi relative alle condizioni della politica per AWS Audit Manager

Supporta le chiavi di condizione delle policy specifiche del servizio	Parziale

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Quando il principale in un'istruzione della policy è un AWS principale del servizio, consigliamo vivamente di utilizzare le chiavi di condizione globale `aws:SourceArn` o `aws:SourceAccount` nella policy. È possibile utilizzare queste chiavi di contesto relative alla condizione globale per evitare lo scenario "deputy confused". Le seguenti policy documentate mostrano il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` in Gestione audit per prevenire il problema confused deputy.

- Policy di esempio per un argomento SNS utilizzato per le notifiche di Gestione audit
- Esempio di policy per una chiave KMS utilizzata con un argomento SNS

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere a un utente l'autorizzazione per accedere a una risorsa solo se è stata taggata con il proprio nome utente. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente IAM.

Gestione audit non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Liste di controllo degli accessi (ACL) in AWS Audit Manager

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con AWS Audit Manager

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'etichettatura AWS Audit Manager delle risorse, consultaTaggare le risorse AWS Audit Manager.

Utilizzo di credenziali temporanee con AWS Audit Manager

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per AWS Audit Manager

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS Audit Manager

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità AWS Audit Manager . Modifica i ruoli del servizio solo quando Gestione audit fornisce le indicazioni per farlo.

Ruoli collegati ai servizi per AWS Audit Manager

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sui ruoli collegati al servizio per, consulta. AWS Audit ManagerUtilizzo di ruoli collegati ai servizi per AWS Audit Manager

Esempi di policy basate sull'identità per AWS Audit Manager

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Gestione audit. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'API. AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Gestione audit AWS, incluso il formato degli ARN per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per Gestione audit AWS in Guida di riferimento per l'autorizzazione del servizio.

Indice

  - Esempio 5 (Autorizzazioni per disabilitare Evidence Finder)
- Consentire l'accesso alla gestione degli utenti a AWS Audit Manager
- Consenti agli utenti l'accesso in sola lettura a AWS Audit Manager
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Consenti AWS Audit Manager l'invio di notifiche agli argomenti di Amazon SNS
  - Esempio 1 (Autorizzazioni per l'argomento SNS)
  - Esempio 2 (Autorizzazioni per la chiave KMS allegata all'argomento SNS)
- Consenti agli utenti di eseguire query di ricerca in Evidence Finder

Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Gestione audit nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla

sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Consenti le autorizzazioni minime richieste per abilitare Gestione audit

In questo esempio viene illustrato come consentire l'attivazione di account senza ruolo di amministratore per abilitare AWS Audit Manager.

> **Note**
>
> Ciò che forniamo qui è una policy di base che concede le autorizzazioni minime necessarie per abilitare Gestione audit. Sono necessarie tutte le autorizzazioni previste nella seguente policy. Se ometti una parte di questa policy non potrai più abilitare Gestione audit.
> Ti consigliamo di dedicare del tempo alla personalizzazione delle autorizzazioni in modo che soddisfino le tue esigenze specifiche. Per ulteriore assistenza, contatta l'amministratore o il Supporto AWS.

Per concedere l'accesso minimo richiesto per abilitare Gestione audit, utilizza le seguenti autorizzazioni.

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

```
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che si sta cercando di eseguire.

Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager

I seguenti criteri di esempio concedono l'accesso amministrativo completo a AWS Audit Manager.

- Esempio 1 (Policy gestita, `AWSAuditManagerAdministratorAccess`)
- Esempio 2 (autorizzazioni di destinazione del rapporto di valutazione)
- Esempio 3 (autorizzazioni di esportazione di destinazione)
- Esempio 4 (Autorizzazioni per abilitare Evidence Finder)
- Esempio 5 (Autorizzazioni per disabilitare Evidence Finder)

Esempio 1 (Policy gestita, **`AWSAuditManagerAdministratorAccess`**)

La AWSAuditManagerAdministratorAccesspolicy include la possibilità di abilitare e disabilitare Audit Manager, la possibilità di modificare le impostazioni di Audit Manager e la possibilità di gestire tutte le risorse di Audit Manager come valutazioni, framework, controlli e report di valutazione.

Esempio 2 (autorizzazioni di destinazione del rapporto di valutazione)

Questa policy ti concede l'autorizzazione ad accedere a uno specifico bucket S3 e ad aggiungere ed eliminare file dallo stesso. Ciò consente di utilizzare il bucket specificato come destinazione del rapporto di valutazione in Gestione audit.

Sostituisci il *`testo segnaposto`* con le tue informazioni. Includi il bucket S3 che utilizzi come destinazione del rapporto di valutazione e la chiave KMS che utilizzi per crittografare i report di valutazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
```

```
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Esempio 3 (autorizzazioni di esportazione di destinazione)

La seguente politica consente di CloudTrail fornire i risultati delle query di Evidence Finder al bucket S3 specificato. Come best practice di sicurezza, la chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la CloudTrail scrittura nel bucket S3 sia utilizzata solo per il data store degli eventi.

Sostituisci il *`testo segnaposto`* con le tue informazioni come segue:

- Sostituisci DOC-EXAMPLE-DESTINATION-BUCKET con il bucket S3 che utilizzi come destinazione di esportazione.
- Sostituisci *`myQueryRunningRegion`* con quello appropriato Regione AWS per la tua configurazione.
- Sostituisci *`myAccountID`* con l' Account AWS ID utilizzato per. CloudTrail Potrebbe non essere lo stesso ID Account AWS per il bucket S3. Se si tratta di un archivio dati di eventi organizzativi, è necessario utilizzare l'archivio Account AWS per l'account di gestione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
```

```
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio 4 (Autorizzazioni per abilitare Evidence Finder)

La seguente policy di autorizzazione è obbligatoria se desideri abilitare e utilizzare la funzionalità di ricerca delle prove. Questa dichiarazione politica consente all'Audit Manager di creare un archivio dati di eventi CloudTrail Lake ed eseguire query di ricerca.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
```

```
                "cloudtrail:CreateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Esempio 5 (Autorizzazioni per disabilitare Evidence Finder)

Questa policy di esempio concede l'autorizzazione a disabilitare la funzionalità Evidence Finder in Gestione audit. Ciò comporta l'eliminazione dell'archivio di dati degli eventi creato quando la funzionalità è stata abilitata per la prima volta.

Per utilizzare questa policy, sostituisci il *testo segnaposto* con le tue informazioni. È necessario specificare l'UUID dell'archivio di dati degli eventi creato quando è stato abilitato Evidence Finder. Puoi recuperare l'ARN del datastore di eventi dalle tue impostazioni di Gestione audit. Per ulteriori informazioni, consulta GetSettingsl'AWS Audit Manager API Reference.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Consentire l'accesso alla gestione degli utenti a AWS Audit Manager

In questo esempio viene illustrato come consentire l'accesso alla gestione non amministrativa a AWS Audit Manager.

Questa policy garantisce la possibilità di gestire tutte le risorse di Gestione audit (valutazioni, framework e controlli), ma non garantisce la possibilità di abilitare o disabilitare Gestione audit o di modificare le impostazioni di Gestione audit.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
```

```
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
"controlcatalog:ListCommonControls",
"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
    ],
    "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Consenti agli utenti l'accesso in sola lettura a AWS Audit Manager

Questa politica garantisce l'accesso in sola lettura a AWS Audit Manager risorse quali valutazioni, framework e controlli.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Consenti AWS Audit Manager l'invio di notifiche agli argomenti di Amazon SNS

Le policy in questo esempio concedono autorizzazioni Gestione audit per inviare notifiche a un argomento Amazon SNS esistente.

- Esempio 1 — Se desideri ricevere notifiche da Audit Manager, usa questo esempio per aggiungere autorizzazioni alla tua politica di accesso agli argomenti SNS.
- Esempio 2: se l'argomento SNS utilizza AWS Key Management Service (AWS KMS) per la crittografia lato server (SSE), utilizza questo esempio per aggiungere autorizzazioni alla politica di accesso tramite chiave KMS.

Nelle seguenti policy, il principale che ottiene le autorizzazioni è il principale del servizio Gestione audit, ovvero `auditmanager.amazonaws.com`. Quando il principale in un'istruzione della policy è un AWS principale del servizio, consigliamo vivamente di utilizzare le chiavi di condizione globale `aws:SourceArn` o `aws:SourceAccount` nella policy. È possibile utilizzare queste chiavi di contesto relative alla condizione globale per evitare lo scenario "deputy confused".

Esempio 1 (Autorizzazioni per l'argomento SNS)

Questa policy consente a Gestione audit di pubblicare eventi sull'argomento SNS specificato. Qualsiasi richiesta di pubblicazione sull'argomento SNS specificato deve soddisfare le condizioni della policy.

Prima di utilizzare questa policy, sostituisci il *testo segnaposto* con le tue informazioni. Prendi nota di quanto segue:

- Se utilizzi la chiave di condizione `aws:SourceArn` in questa policy, il valore deve essere l'ARN della risorsa Gestione audit da cui proviene la notifica. Nell'esempio seguente, `aws:SourceArn` utilizza un carattere jolly (*) per l'ID della risorsa. Ciò consente tutte le richieste provenienti da Gestione audit su tutte le risorse di Gestione audit. Con la chiave di condizione globale `aws:SourceArn`, puoi utilizzare l'operatore di condizione `StringLike` o `ArnLike`. Come best practice, ti suggeriamo di utilizzare `ArnLike`.
- Con la chiave di condizione globale `aws:SourceAccount`, puoi utilizzare l'operatore di condizione `StringEquals` o `StringLike`. Come best practice, consigliamo di usare `StringEquals` per implementare il privilegio minimo.
- Se utilizzi sia `aws:SourceAccount` che `aws:SourceArn`, i valori account devono mostrare lo stesso ID account.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
```

```
}
```

L'esempio seguente utilizza solo la chiave di condizione `aws:SourceArn` con l'operatore di condizione `StringLike`:

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
      }
    }
```

L'esempio seguente utilizza solo la chiave di condizione `aws:SourceAccount` con l'operatore di condizione `StringLike`:

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
  }
```

Esempio 2 (Autorizzazioni per la chiave KMS allegata all'argomento SNS)

Questa policy permette a Gestione audit di utilizzare la chiave KMS per generare la chiave dati che usa per crittografare un argomento SNS. Qualsiasi richiesta di utilizzare la chiave KMS per l'operazione specificata deve soddisfare le condizioni di questa policy.

Prima di utilizzare questa policy, sostituisci il *testo segnaposto* con le tue informazioni. Prendi nota di quanto segue:

- Se utilizzi la chiave di condizione `aws:SourceArn` in questa policy, il valore deve essere l'ARN della risorsa che viene crittografata. Ad esempio, in questo caso, è l'argomento SNS del tuo account. Imposta il valore sull'ARN o un modello ARN con caratteri jolly (*). Con la chiave di condizione globale `aws:SourceArn` puoi utilizzare l'operatore di condizione `StringLike` o `ArnLike`. Come best practice, ti suggeriamo di utilizzare `ArnLike`.
- Con la chiave di condizione globale `aws:SourceAccount`, puoi utilizzare l'operatore di condizione `StringEquals` o `StringLike`. Come best practice, consigliamo di usare `StringEquals` per implementare il privilegio minimo. Puoi utilizzare `aws:SourceAccount` se non conosci l'ARN dell'argomento SNS.

- Se utilizzi sia `aws:SourceAccount` che `aws:SourceArn`, i valori account devono mostrare lo stesso ID account.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
       "Condition": {
           "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                 "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

L'esempio seguente utilizza solo la chiave di condizione `aws:SourceArn` con l'operatore di condizione `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

L'esempio seguente utilizza solo la chiave di condizione `aws:SourceAccount` con l'operatore di condizione `StringLike`:

```
   "Condition": {
```

```
     "StringLike": {
       "aws:SourceAccount": "accountID"
      }
    }
```

Consenti agli utenti di eseguire query di ricerca in Evidence Finder

La seguente politica concede le autorizzazioni per eseguire query su un data store di eventi Lake. CloudTrail La presente policy di autorizzazione è obbligatoria se desideri utilizzare la funzionalità di ricerca delle prove.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può causare il confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, Amazon Web Services fornisce strumenti per aiutarti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto `aws:SourceArn`e le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni concesse a un altro servizio per l'accesso alle tue risorse. AWS Audit Manager

- Utilizza `aws:SourceArn`se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Se desideri specificare più risorse, puoi anche usare `aws:SourceArn` con un carattere jolly (*).

  Ad esempio, potresti utilizzare un argomento Amazon SNS per ricevere notifiche di attività da Gestione audit. In questo caso, nella policy di accesso agli argomenti SNS, il valore ARN `aws:SourceArn` è la risorsa Gestione audit da cui proviene la notifica. Poiché è probabile che tu disponga di più risorse Gestione audit, ti consigliamo di utilizzare `aws:SourceArn` con un carattere jolly. In questo modo puoi specificare tutte le risorse di Gestione audit nella policy di accesso agli argomenti SNS.
- Utilizza `aws:SourceAccount`se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.
- Se il valore `aws:SourceArn`non contiene l'ID account, ad esempio un ARN del bucket Amazon S3, devi utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni.
- Se utilizzi entrambe le condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account quando viene utilizzato nella stessa dichiarazione di policy.
- Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci il nome della risorsa Amazon (ARN) completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Supporto confused deputy Gestione audit

Gestione audit fornisce un supporto confused deputy nei seguenti scenari. Gli esempi di policy seguenti mostrano il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` per prevenire il problema confused deputy.

- Policy di esempio: l'argomento SNS utilizzato per ricevere le notifiche di Gestione audit
- Policy di esempio: la chiave KMS che usi per crittografare il tuo argomento SNS

Gestione audit non fornisce un supporto confused deputy per la chiave gestita dal cliente fornita nelle impostazioni Configurazione delle impostazioni di crittografia dei dati di Gestione audit. Se hai fornito la tua chiave gestita dal cliente, non puoi utilizzare le condizioni `aws:SourceAccount` o `aws:SourceArn`contenute in tale policy della chiave KMS.

AWS politiche gestite per AWS Audit Manager

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.

Argomenti

- AWS politica gestita: AWSAuditManagerAdministratorAccess
- AWS politica gestita: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager aggiornamenti alle politiche AWS gestite

AWS politica gestita: AWSAuditManagerAdministratorAccess

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

Questa politica concede autorizzazioni amministrative che consentono l'accesso amministrativo completo a. AWS Audit Manager Questo accesso include la possibilità di abilitare e disabilitare AWS Audit Manager, modificare le impostazioni e gestire tutte le risorse di Audit Manager come valutazioni, framework, controlli e report di valutazione. AWS Audit Manager

AWS Audit Manager richiede ampie autorizzazioni per più servizi. AWS Questo perché si AWS Audit Manager integra con più AWS servizi per raccogliere automaticamente le prove dai servizi Account AWS e dai servizi oggetto di una valutazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `Audit Manager`: consente ai responsabili le autorizzazioni complete sulle risorse AWS Audit Manager .
- `Organizations`: consente ai responsabili di elencare gli account e le unità organizzative e di registrare o annullare la registrazione di un amministratore delegato. Ciò è necessario per abilitare il supporto per più account e consentire di AWS Audit Manager eseguire valutazioni su più account e consolidare le prove in un account amministratore delegato.
- `iam`: consente ai principali di ottenere ed elencare gli utenti in IAM e creare un ruolo collegato ai servizi. Ciò è necessario per poter designare i proprietari e i delegati dell'audit per una valutazione. Inoltre, questa policy consente ai principali di eliminare il ruolo collegato al servizio e recuperare lo stato di eliminazione. Ciò è necessario per AWS Audit Manager poter ripulire le risorse ed eliminare automaticamente il ruolo collegato al servizio quando si sceglie di disabilitare il servizio in. AWS Management Console
- `s3`: consente ai principali di elencare i bucket Amazon Simple Storage Service (Amazon S3) disponibili. Questa funzionalità è necessaria per poter designare il bucket S3 in cui archiviare i report relativi alle prove o caricare prove manuali.
- `kms`: consente ai responsabili di elencare e descrivere chiavi, elencare alias e creare sovvenzioni. Ciò è necessario per poter scegliere le chiavi gestite dal cliente per la crittografia dei dati.
- `sns`: consente ai responsabili di elencare gli argomenti relativi agli abbonamenti in Amazon SNS. Ciò è necessario per specificare a quale argomento SNS desideri che AWS Audit Manager invii le notifiche.
- `events`— Consente ai responsabili di elencare e gestire i controlli da. AWS Security Hub Ciò è necessario per AWS Audit Manager poter raccogliere automaticamente AWS Security Hub i risultati per i AWS servizi monitorati da AWS Security Hub. Può quindi convertire questi dati in prove da includere nelle tue valutazioni AWS Audit Manager .
- `tag`: consente ai presidi di recuperare le risorse contrassegnate. Ciò è necessario per poter utilizzare i tag come filtro di ricerca durante l'esplorazione di framework, controlli e valutazioni in AWS Audit Manager.

- `controlcatalog`— Consente ai responsabili di elencare i domini, gli obiettivi e i controlli comuni forniti da AWS Control Catalog. Ciò è necessario per poter utilizzare la funzionalità dei controlli comuni in. AWS Audit Manager Con queste autorizzazioni, è possibile visualizzare un elenco di controlli comuni nella libreria dei AWS Audit Manager controlli e filtrare i controlli per dominio e obiettivo. Puoi anche utilizzare i controlli comuni come fonte di evidenza quando crei un controllo personalizzato.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
     "Sid": "ControlCatalogAccess",
     "Effect": "Allow",
     "Action": [
  "controlcatalog:ListCommonControls",
  "controlcatalog:ListDomains",
  "controlcatalog:ListObjectives"
     ],
     "Resource": "*"
```

```
        }
    ]
}
```

AWS politica gestita: AWSAuditManagerServiceRolePolicy

Non è possibile collegare `AWSAuditManagerServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato al servizio`AWSServiceRoleForAuditManager`, che consente di eseguire azioni AWS Audit Manager per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS Audit Manager.

La policy sulle autorizzazioni dei ruoli, `AWSAuditManagerServiceRolePolicy`, consente a AWS Audit Manager di raccogliere prove automatiche eseguendo le seguenti operazioni per tuo conto:

- Raccogli i dati delle seguenti origini dati:
  - Eventi di gestione da AWS CloudTrail
  - Controlli di conformità da Regole di AWS Config
  - Controlli di conformità da AWS Security Hub
- Utilizza le chiamate API per descrivere le configurazioni delle risorse per i seguenti Servizi AWS.

> **Tip**
>
> Per ulteriori informazioni sulle chiamate API utilizzate da Gestione audit per raccogliere prove da questi servizi, consulta Chiamate API supportate per fonti di dati di controllo personalizzate in questa guida.

  - Amazon API Gateway
  - AWS Backup
  - Amazon Bedrock
  - AWS Certificate Manager
  - Amazon CloudFront
  - AWS CloudTrail
  - Amazon CloudWatch
  - CloudWatch Registri Amazon
  - Pool di utenti Amazon Cognito

- AWS Config
- Amazon Data Firehose
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Dimensionamento automatico Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Sistema di bilanciamento del carico elastico
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming per Apache Kafka
- OpenSearch Servizio Amazon
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Secrets Manager

- AWS Security Hub

- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Dettagli dell'autorizzazione

`AWSAuditManagerServiceRolePolicy`consente AWS Audit Manager di completare le seguenti azioni sulle risorse specificate:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`
- `cloudtrail:ListTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`

- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules

- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule

- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy

- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups

- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - Questa azione API opera nell'ambito di Account AWS dove service-linked-role è disponibile. Non può accedere alle policy relative ai bucket su più account.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm

- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets

- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
```

```
    "bedrock:ListModelCustomizationJobs",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListDistributions",
    "cloudtrail:GetTrail",
    "cloudtrail:ListTrails",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeBackup",
    "dynamodb:DescribeTableReplicaAutoScaling",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeInstanceCreditSpecifications",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeVpcEndpointConnections",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:GetLaunchTemplateData",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
```

```
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccessKeyLastUsed",
    "iam:GetCredentialReport",
    "iam:GetGroupPolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetUserPolicy",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:ListAttachedGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListEntitiesForPolicy",
```

```
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "iam:ListPolicyVersions",
    "iam:ListAccessKeys",
    "iam:ListAttachedRolePolicies",
    "iam:ListMfaDeviceTags",
    "iam:ListMfaDevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "logs:GetDataProtectionPolicy",
    "es:DescribeDomains",
    "es:DescribeDomain",
    "es:DescribeDomainConfig",
    "es:ListDomainNames",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterEndpoints",
```

```
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstances",
    "rds:DescribeDBSecurityGroups",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeLoggingStatus",
    "route53:GetQueryLoggingConfig",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:DescribeFlowDefinition",
    "sagemaker:DescribeHumanTaskUi",
    "sagemaker:DescribeModelBiasJobDefinition",
    "sagemaker:DescribeModelCard",
    "sagemaker:DescribeModelQualityJobDefinition",
    "sagemaker:DescribeDomain",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeLabelingJob",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListAlgorithms",
    "sagemaker:ListDomains",
    "sagemaker:ListEndpoints",
    "sagemaker:ListEndpointConfigs",
    "sagemaker:ListFlowDefinitions",
    "sagemaker:ListHumanTaskUis",
    "sagemaker:ListLabelingJobs",
    "sagemaker:ListModels",
    "sagemaker:ListModelBiasJobDefinitions",
    "sagemaker:ListModelCards",
    "sagemaker:ListModelQualityJobDefinitions",
    "sagemaker:ListMonitoringAlerts",
    "sagemaker:ListMonitoringSchedules",
    "sagemaker:ListTrainingJobs",
    "sagemaker:ListUserProfiles",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:ListSecrets",
```

```
    "securityhub:DescribeStandards",
    "sns:ListTagsForResource",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetRule",
    "waf-regional:GetWebAcl",
    "waf:GetRule",
    "waf:GetRuleGroup",
    "waf:ListActivatedRulesInRuleGroup",
    "waf:ListWebAcls",
    "wafv2:ListWebAcls",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf-regional:ListRules",
    "waf:ListRuleGroups",
    "waf:ListRules"
   ],
   "Resource": "*",
   "Sid": "APIsAccess"
  },
  {
   "Sid": "S3Access",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketAcl",
    "s3:GetBucketLogging",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketTagging"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "APIGatewayAccess",
   "Effect": "Allow",
```

```
    "Action": [
     "apigateway:GET"
    ],
    "Resource": [
     "arn:aws:apigateway:*::/restapis",
     "arn:aws:apigateway:*::/restapis/*/stages/*",
     "arn:aws:apigateway:*::/restapis/*/stages"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": [
       "${aws:PrincipalAccount}"
      ]
     }
    }
   },
   {
    "Sid": "CreateEventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
    "Condition": {
     "StringEquals": {
      "events:detail-type": "Security Hub Findings - Imported"
     },
     "Null": {
      "events:source": "false"
     },
     "ForAllValues:StringEquals": {
      "events:source": [
       "aws.securityhub"
      ]
     }
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
```

```
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  }
 ]
}
```

AWS Audit Manager aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Audit Manager 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 Audit Manager documenti.

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy: aggiornamento a una policy esistente	Abbiamo aggiunto le seguenti autorizzazioni a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ora puoi eseguire le seguenti azioni per raccogliere prove automatiche sulle risorse del tuo Account AWS. • `sagemaker:DescribeAlgorithm` • `sagemaker:DescribeDomain` • `sagemaker:DescribeEndpoint` • `sagemaker:DescribeFlowDefinition` • `sagemaker:DescribeHumanTaskUi` • `sagemaker:DescribeLabelingJob` • `sagemaker:DescribeModel` • `sagemaker:DescribeModelBiasJobDefinition` • `sagemaker:DescribeModelCard`	10/06/2024

Modifica	Descrizione	Data
	• sagemaker:DescribeModelQualityJobDefinition • sagemaker:DescribeTrainingJob • sagemaker:DescribeUserProfile • sagemaker:ListAlgorithms • sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels • sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy: aggiornamento a una policy esistente	Abbiamo aggiunto le seguenti autorizzazioni a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ora puoi eseguire le seguenti azioni per raccogliere prove automatiche sulle risorse del tuo Account AWS. • `iam:ListAttachedGroupPolicies` • `iam:ListAttachedUserPolicies` • `iam:ListGroupsForUser` • `es:ListDomainNames` Abbiamo anche aggiunto una nuova risorsa nella `APIGatewayAccess` sezione della politica (`arn:aws:apigateway:*::/restapis`). La policy ora concede l'autorizzazione specificata (in questo caso, l'`apigateway:GET` azione) non solo sulle fasi e sulle risorse di fase delle API REST di API Gateway, ma anche sulle API REST stesse. Questa modifica amplia efficacemente l'ambito della policy per includere la possibilità di recuperare informazioni sulle stesse API REST di API Gateway, oltre alle fasi e alle risorse di fase associate a tali API.	17/05/2024

Modifica	Descrizione	Data
AWSAuditManagerAdministratorAccess: aggiornamento a una policy esistente	Abbiamo aggiunto la seguenti autorizzazione relativa a `AWSAuditManagerAdministratorAccess` : • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` Questo aggiornamento consente di visualizzare i domini di controllo, gli obiettivi di controllo e i controlli comuni forniti da Control Catalog. AWS Queste autorizzazioni sono necessarie se si desidera utilizzare la funzionalità dei controlli comuni in. AWS Audit Manager	15/05/2024

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy : aggiornamento a una policy esistente	Abbiamo aggiunto le seguenti autorizzazioni a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ora puoi eseguire le seguenti azioni per raccogliere prove automatiche sulle risorse del tuo Account AWS. • `apigateway:GET` • `autoscaling:DescribeAutoScalingGroups` • `backup:ListBackupPlans` • `cloudfront:GetDistribution` • `cloudfront:GetDistributionConfig` • `cloudfront:ListDistributions` • `cloudtrail:GetTrail` • `cloudtrail:ListTrails` • `dynamodb:DescribeContinuousBackups` • `dynamodb:DescribeBackup` • `dynamodb:DescribeTableReplicaAutoScaling` • `ec2:DescribeInstanceCreditSpecifications` • `ec2:DescribeInstanceAttribute` • `ec2:DescribeSecurityGroupRules` • `ec2:DescribeVpcEndpointConnections` • `ec2:DescribeVpcEndpointServiceConfigurations` • `ec2:GetLaunchTemplateData` • `es:DescribeDomains`	15/05/2024

Modifica	Descrizione	Data
	• es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig • sagemaker:ListEndpointConfigs	

Modifica	Descrizione	Data
	• `secretsmanager:DescribeSecret` • `secretsmanager:ListSecrets` • `sns:ListTagsForResource` • `waf-regional:GetRule` • `waf-regional:GetWebAcl` • `waf-regional:ListRules` • `waf:GetRule` • `waf:GetRuleGroup` • `waf:ListRuleGroups` • `waf:ListRules` • `waf:ListWebAcls` • `wafv2:ListWebAcls`	
AWSAuditManagerServiceRolePolicy : aggiornamento a una policy esistente	Il ruolo collegato al servizio ora consente AWS Audit Manager di eseguire l'azione. `s3:GetBucketPolicy` Questa operazione API è necessaria per supportare il framework delle best practice AWS per l'IA generativa v1. Consente a Gestione audit di raccogliere prove automatiche sulle restrizioni delle policy in vigore per i set di dati di addestramento dei modelli di IA generativa. L'`GetBucketPolicy` azione opera nell'ambito di Account AWS dove service-linked-role è disponibile. Non può accedere alle policy relative ai bucket su più account.	12/06/2023

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy : aggiornamento a una policy esistente	Abbiamo aggiunto le seguenti autorizzazioni a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ora puoi eseguire le seguenti azioni per raccogliere prove automatiche sulle risorse del tuo Account AWS. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizationJob` • `bedrock:GetModelInvocationLoggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels` • `bedrock:ListModelCustomizationJobs` • `cloudtrail:LookupEvents` • `cloudwatch:DescribeAlarmsForMetric` • `cloudwatch:GetMetricStatistics` • `cloudwatch:ListMetrics` • `directconnect:DescribeDirectConnectGateways` • `directconnect:DescribeVirtualGateways` • `dynamodb:ListBackups` • `dynamodb:ListGlobalTables`	11/06/2023

Modifica	Descrizione	Data
	• ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers • elasticloadbalancing:DescribeSslPolicies	

Modifica	Descrizione	Data
	• elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints	

Modifica	Descrizione	Data
	• rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy : aggiornamento a una policy esistente	Abbiamo aggiunto la seguenti autorizzazione relativa a AWSAuditManagerServiceRolePolicy : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy: aggiornamento a una policy esistente	Il ruolo collegato al servizio ora consente di AWS Audit Manager eseguire l'azione. `organizations:DescribeOrganization` Abbiamo anche suddiviso la risorsa `CreateEventsAccess` da un carattere jolly (*) a un tipo specifico di risorsa (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Infine, abbiamo aggiunto un operatore di condizione `Null` per la chiave di condizione `events:source` per confermare che esiste un valore di origine e che il suo valore non è nullo.	20/05/2022
AWSAuditManagerAdministratorAccess: aggiornamento a una policy esistente	Abbiamo aggiornato la policy delle condizioni chiave per `events:source` per indicare che si tratta di una chiave multivalore.	29/04/2022
AWSAuditManagerServiceRolePolicy: aggiornamento a una policy esistente	Abbiamo aggiornato la policy delle condizioni chiave per `events:source` per indicare che si tratta di una chiave multivalore.	16/03/2022
AWS Audit Manager ha iniziato a tenere traccia delle modifiche	AWS Audit Manager ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	05/06/2021

Risoluzione dei problemi relativi all' AWS Audit Manager identità e all'accesso

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Gestione audit e di IAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione in AWS Audit Manager

L'`AccessDeniedException`errore viene visualizzato quando un utente non dispone dell'autorizzazione per utilizzare AWS Audit Manager o le operazioni dell'API Audit Manager.

In questo caso, il tuo amministratore deve aggiornare la policy per consentirti l'accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Gestione audit.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente esempio di errore si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Gestione audit. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Audit Manager risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Gestione audit supporta queste funzionalità, consulta Come AWS Audit Manager funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Utilizzo di ruoli collegati ai servizi per AWS Audit Manager

AWS Audit Manager utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a Gestione audit. I ruoli collegati ai servizi sono predefiniti da Audit Manager e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione AWS Audit Manager perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Gestione audit definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo Gestione audit potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per AWS Audit Manager

Audit Manager utilizza il ruolo collegato ai servizi denominato**`AWSServiceRoleForAuditManager`**, che consente l'accesso ai servizi e alle risorse AWS utilizzati o gestiti da. AWS Audit Manager

Ai fini dell'assunzione del ruolo `AWSServiceRoleForAuditManager`, il ruolo collegato ai servizi `auditmanager.amazonaws.com`considera attendibile il servizio.

La politica di autorizzazione dei ruoli consente all'Audit Manager di raccogliere prove automatiche sull' AWS utilizzo da parte dell'utente. `AWSAuditManagerServiceRolePolicy` In particolare, può effettuare le operazioni seguenti per conto tuo.

- Audit Manager può essere utilizzato AWS Security Hub per raccogliere prove di verifica della conformità. In questo caso, Audit Manager utilizza la seguente autorizzazione per riportare i risultati dei controlli di sicurezza direttamente da AWS Security Hub. Quindi allega i risultati ai controlli di valutazione pertinenti come prove.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Per ulteriori informazioni su quali controlli specifici del Security Hub Gestione audit può descrivere, consulta i AWS Security Hub controlli supportati da AWS Audit Manager.

- Audit Manager può essere utilizzato AWS Config per raccogliere prove di verifica della conformità. In questo caso, Audit Manager utilizza le seguenti autorizzazioni per riportare i risultati delle valutazioni delle AWS Config regole direttamente da AWS Config. Quindi allega i risultati ai controlli di valutazione pertinenti come prove.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

> **Note**
>
> Per ulteriori informazioni sulle AWS Config regole specifiche che Audit Manager può descrivere, vedere AWS Config Regole supportate da AWS Audit Manager.

- Audit Manager può essere utilizzato AWS CloudTrail per raccogliere prove delle attività degli utenti. In questo caso, Audit Manager utilizza le seguenti autorizzazioni per acquisire l'attività dell'utente dai CloudTrail log. Quindi allega i l'attività ai controlli di valutazione pertinenti come prove.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Per ulteriori informazioni sugli CloudTrail eventi specifici che Audit Manager può descrivere, vedere i nomi AWS CloudTrail degli eventi supportati da AWS Audit Manager.

- Audit Manager può utilizzare le chiamate AWS API per raccogliere prove di configurazione delle risorse. In questo caso, Gestione audit utilizza le seguenti autorizzazioni per richiamare API di sola lettura che descrivono le configurazioni delle risorse per i seguenti Servizi AWS. Quindi allega le risposte API ai controlli di valutazione pertinenti come prove.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`

- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute

- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers

- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy

- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus

- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls

- s3:GetBucketPolicy
  - Questa azione API opera nell'ambito di Account AWS dove service-linked-role è disponibile. Non può accedere alle policy relative ai bucket su più account.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels

- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

> **Note**
>
> Per ulteriori informazioni sulle chiamate API specifiche che Gestione audit può descrivere, consulta Chiamate API supportate per fonti di dati di controllo personalizzate.

Per visualizzare i dettagli completi delle autorizzazioni del ruolo collegato al servizio`AWSServiceRoleForAuditManager`, consulta la AWS Managed Policy AWSAuditManagerServiceRolePolicyReference Guide.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio AWS Audit Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando lo abiliti AWS Audit Manager, il servizio crea automaticamente il ruolo collegato al servizio per te. È possibile abilitare Audit Manager dalla pagina di onboarding di AWS Management Console, o tramite l'API o. AWS CLI Per ulteriori informazioni, consulta Abilitazione AWS Audit Manager nella Guida per l'utente.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account.

Modifica del ruolo collegato al servizio AWS Audit Manager

AWS Audit Manager non consente di modificare il ruolo collegato al `AWSServiceRoleForAuditManager` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Consentire a un'entità IAM di modificare la descrizione del ruolo collegato ai servizi **`AWSServiceRoleForAuditManager`**

Aggiungi la seguente istruzione alla policy delle autorizzazioni per l'entità IAM che deve modificare la descrizione di un ruolo collegato ai servizi.

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Eliminazione del ruolo collegato al servizio AWS Audit Manager

Se non devi più utilizzare Gestione audit, è consigliabile eliminare il ruolo collegato ai servizi `AWSServiceRoleForAuditManager`. In questo modo, non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, devi effettuare la pulizia del ruolo collegato ai servizi prima di poterlo eliminare.

Pulizia del ruolo collegato ai servizi

Prima di utilizzare IAM per eliminare un ruolo collegato ai servizi Gestione audit, devi innanzitutto verificare che il ruolo non abbia sessioni attive ed eliminare tutte le risorse utilizzate dal ruolo. A tal fine, assicurati che Audit Manager sia completamente cancellato. Regioni AWS Dopo l'annullamento della registrazione, Gestione audit non utilizza più il ruolo collegato al servizio.

Per istruzioni su come annullare la registrazione Gestione audit, consulta le seguenti risorse:

- Disabilitazione AWS Audit Manager in questa guida
- DeregisterAccount nel documento di riferimento delle API AWS Audit Manager
- deregister-account nel Reference per AWS CLI AWS Audit Manager

Per istruzioni su come eliminare manualmente le risorse di Gestione audit, consulta Eliminazione dei dati di Gestione audit in questa guida.

Eliminazione del ruolo collegato ai servizi

Puoi eliminare il ruolo collegato ai servizi tramite la console IAM, AWS Command Line Interface (AWS CLI), o tramite API IAM.

IAM console

Segui questi passaggi per eliminare il ruolo collegato ai servizi tramite la console IAM.

Per eliminare un ruolo collegato ai servizi (console)

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM seleziona Ruoli. Quindi seleziona la casella di controllo accanto a `AWSServiceRoleForAuditManager`, non il nome o la riga.
3. Nella sezione Operazioni ruolo nella parte superiore della pagina, seleziona Elimina.
4. Nella finestra di dialogo di conferma controlla le informazioni relative all'ultimo accesso che indicano quando ognuno dei ruoli selezionati ha effettuato l'accesso a un servizio Servizio AWS. In questo modo potrai verificare se il ruolo è attualmente attivo. Se desideri procedere, digita **`AWSServiceRoleForAuditManager`** nel campo di inserimento del test e scegli Elimina per richiedere l'eliminazione del ruolo collegato ai servizi.
5. Controlla le notifiche della console IAM per monitorare lo stato dell'eliminazione del ruolo collegato ai servizi. Poiché l'eliminazione del ruolo collegato ai servizi IAM è asincrona, una volta richiesta l'eliminazione del ruolo, il task di eliminazione può essere eseguito correttamente o meno. Se il task viene eseguito correttamente, il ruolo viene rimosso dall'elenco e nella parte superiore della pagina viene visualizzato un messaggio di completamento.

AWS CLI

Puoi utilizzare i comandi IAM di AWS CLI per eliminare un ruolo collegato al servizio.

Per eliminare un ruolo collegato ai servizi (AWS CLI)

1. Inserisci il comando seguente per elencare il ruolo nel tuo account:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Poiché un ruolo collegato ai servizi non può essere eliminato se è in uso o se a esso sono associate delle risorse, occorre inviare una richiesta di eliminazione. Se queste condizioni non sono soddisfatte, la richiesta può essere rifiutata. Acquisisci il valore di `deletion-task-id`dalla risposta per controllare lo stato del task di eliminazione.

   Per inviare una richiesta di eliminazione per un ruolo collegato ai servizi, digita il seguente comando:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Digita il seguente comando per verificare lo stato del processo di eliminazione:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

Lo stato di un task di eliminazione può essere `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`o `FAILED`. Se l'eliminazione non viene eseguita correttamente, la chiamata restituisce il motivo dell'errore per consentire all'utente di risolvere il problema.

IAM API

È possibile utilizzare l'API di IAM; per eliminare un ruolo collegato ai servizi.

Per eliminare un ruolo collegato ai servizi (API)

1. Chiama GetRoleper elencare il ruolo nel tuo account. Nella richiesta, specifica `AWSServiceRoleForAuditManager` come `RoleName`.
2. Poiché un ruolo collegato ai servizi non può essere eliminato se è in uso o se a esso sono associate delle risorse, occorre inviare una richiesta di eliminazione. Se queste condizioni non sono soddisfatte, la richiesta può essere rifiutata. Acquisisci il valore di `DeletionTaskId`dalla risposta per controllare lo stato del task di eliminazione.

   Per inviare una richiesta di eliminazione per un ruolo collegato al servizio, chiama. DeleteServiceLinkedRole Nella richiesta, specifica `AWSServiceRoleForAuditManager` come `RoleName`.
3. Per verificare lo stato dell'eliminazione, chiama. GetServiceLinkedRoleDeletionStatus Nella richiesta, specificare il `DeletionTaskId`.

   Lo stato di un task di eliminazione può essere `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED`o `FAILED`. Se l'eliminazione non viene eseguita correttamente, la chiamata restituisce il motivo dell'errore per consentire all'utente di risolvere il problema.

Suggerimenti per l'eliminazione del ruolo collegato al servizio Audit Manager

Il processo di eliminazione per il ruolo collegato al servizio Audit Manager potrebbe non riuscire se Audit Manager utilizza il ruolo o dispone di risorse associate. Ciò può verificarsi nei seguenti scenari:

1. Il tuo account è ancora registrato con Audit Manager in uno o più account Regioni AWS.
2. Il tuo account fa parte di un' AWS organizzazione e l'account di gestione o l'account amministratore delegato è ancora inserito in Audit Manager.

Per risolvere un problema di eliminazione non riuscita, inizia controllando se fai parte di Account AWS un'organizzazione. Puoi farlo chiamando l'operatore dell'DescribeOrganizationAPI o accedendo alla AWS Organizations console.

Se fai Account AWS parte di un'organizzazione

1. Usa il tuo account di gestione per rimuovere l'amministratore delegato in Audit Manager in tutti i Regioni AWS casi in cui ne hai aggiunto uno.
2. Usa il tuo account di gestione per annullare la registrazione di Audit Manager in tutti i Regioni AWS luoghi in cui hai utilizzato il servizio.
3. Riprova a eliminare il ruolo collegato al servizio seguendo i passaggi della procedura precedente.

Se non Account AWS fai parte di un'organizzazione

1. Assicurati di aver annullato la registrazione di Audit Manager in tutte le aree in Regioni AWS cui hai utilizzato il servizio.
2. Riprova a eliminare il ruolo collegato al servizio seguendo i passaggi della procedura precedente.

Dopo aver annullato la registrazione da Audit Manager, il servizio smetterà di utilizzare il ruolo collegato al servizio. È quindi possibile eliminare il ruolo con successo.

Regioni supportate per i ruoli AWS Audit Manager collegati ai servizi

AWS Audit Manager supporta l'utilizzo di ruoli collegati al servizio in tutti i paesi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint del servizio AWS.

Convalida della conformità per AWS Audit Manager

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.

- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Comprendere la resilienza in AWS Audit Manager

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti.

Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS Audit Manager

In quanto servizio gestito, AWS Audit Manager è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad AWS Audit Manager attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.

- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi chiamare queste operazioni API da qualsiasi posizione di rete, ma AWS Audit Manager supporta politiche di accesso basate sulle risorse, che possono includere restrizioni basate sull'indirizzo IP di origine. Inoltre, è possibile utilizzare le policy Gestione audit per controllare l'accesso da endpoint Amazon Virtual Private Cloud (Amazon VPC) o VPC specifici. In effetti, questo isola l'accesso alla rete a una determinata risorsa Audit Manager solo dal VPC specifico all'interno AWS della rete.

AWS Audit Manager e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e creare un AWS Audit Manager endpoint VPC di interfaccia. Gli endpoint dell'interfaccia sono basati su AWS PrivateLink, una tecnologia che consente di accedere privatamente alle API Gestione audit senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect. Le istanze presenti nel VPC non richiedono indirizzi IP pubblici per comunicare con le API di Gestione audit. Il traffico tra il tuo VPC e AWS Audit Manager non esce dalla AWS rete.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti.

Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Considerazioni sugli endpoint AWS Audit Manager VPC

Prima di configurare un endpoint VPC di interfaccia per AWS Audit Manager, assicurati di esaminare le proprietà e le limitazioni degli endpoint dell'interfaccia nella Amazon VPC User Guide.

AWS Audit Manager supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC.

Creazione di un endpoint VPC interfaccia per l' AWS Audit Manager

Puoi creare un endpoint VPC per il AWS Audit Manager servizio utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per AWS Audit Manager utilizzare il seguente nome di servizio:

- `com.amazonaws.region.auditmanager`

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API AWS Audit Manager utilizzando il nome DNS predefinito per la regione, ad esempio. `auditmanager.us-east-1.amazonaws.com`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint dell'interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy per gli endpoint VPC per AWS Audit Manager

È possibile allegare un criterio all'endpoint VPC che controlla l'accesso all' AWS Audit Manager. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni AWS Audit Manager

Di seguito è riportato un esempio di policy sugli endpoint per. AWS Audit Manager Se collegato a un endpoint, questa policy concede l'accesso alle operazioni Gestione audit elencate per tutti i principali su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
```

```
            "Action":[
               "auditmanager:GetAssessment",
               "auditmanager:GetServicesInScope",
               "auditmanager:ListNotifications"
            ],
            "Resource":"*"
         }
      ]
}
```

Registrazione e monitoraggio AWS Audit Manager

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Audit Manager e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per controllare Audit Manager, segnalare quando qualcosa non va e intraprendere azioni automatiche quando appropriato:

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo Account AWS e fornisce i file di log a un bucket Simple Storage Service (Amazon S3) specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.
- Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, dalle applicazioni oftware-as-a S-Service (SaaS) e dai servizi AWS e indirizza tali dati verso destinazioni come Lambda. In questo modo puoi monitorare gli eventi che si verificano nei servizi e creare architetture basate su eventi. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Monitoraggio AWS Audit Manager con Amazon EventBridge

Amazon ti EventBridge aiuta ad automatizzare Servizi AWS e rispondere automaticamente a eventi di sistema come problemi di disponibilità delle applicazioni o modifiche delle risorse.

È possibile utilizzare EventBridge le regole per rilevare e reagire agli eventi di Audit Manager. In base alle regole create, EventBridge richiama una o più azioni mirate quando un evento corrisponde ai valori specificati in una regola. A seconda del tipo di evento, potresti voler inviare notifiche, acquisire informazioni sull'evento, intraprendere un'azione correttiva, avviare eventi o eseguire altre operazioni.

Ad esempio, puoi rilevare ogni volta che si verificano i seguenti eventi Gestione audit nel tuo account:

- Il proprietario dell'audit crea, aggiorna o elimina una valutazione
- Il proprietario dell'audit delega un set di controlli per la revisione
- Un delegato completa la revisione e invia il set di controlli esaminato al proprietario dell'audit
- Il proprietario di un audit aggiorna lo stato di una valutazione e controllo

Le azioni che possono essere attivate automaticamente includono le seguenti:

- Usa una AWS Lambda funzione per passare una notifica a un canale Slack.
- Immetti dati sui controlli dei flussi di dati Amazon Kinesis per un monitoraggio completo e in tempo reale dello stato.
- Invia un argomento Amazon Simple Notification Service (Amazon SNS) sulla tua e-mail.
- Ricevi una notifica con un'azione di CloudWatch allarme di Amazon.

> **Note**
>
> Gestione audit offre eventi in modo duraturo. Ciò significa che Audit Manager tenterà con successo di fornire gli eventi EventBridge almeno una volta. Nei casi in cui gli eventi non possono essere erogati a causa di un'interruzione del EventBridge servizio, verranno riprovati in seguito da Audit Manager per un massimo di 24 ore.

EventBridge formato di esempio per Audit Manager

Il codice JSON seguente mostra un esempio di evento di creazione di una valutazione in Gestione audit. Per informazioni su uno qualsiasi dei campi di questo evento, consulta Riferimento alla struttura degli eventi.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
```

```
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Prerequisiti per la creazione di una regola EventBridge

Prima di creare regole per gli eventi Gestione audit, ti consigliamo di effettuare le seguenti operazioni:

- Acquisisci familiarità con eventi, regole e obiettivi in. EventBridge Per ulteriori informazioni, consulta What is Amazon EventBridge? nella Amazon EventBridge User Guide.
- Creare la destinazione da utilizzare nella regola degli eventi. Ad esempio, puoi creare un argomento Amazon SNS in modo che ogni volta che viene completata una revisione del set di controlli, riceverai un messaggio di testo o un'e-mail. Per ulteriori informazioni, consulta EventBridge gli obiettivi.

Creazione di una EventBridge regola per Audit Manager

Segui questi passaggi per creare una EventBridge regola che si attiva su un evento emesso da Audit Manager. Gli eventi vengono emessi secondo il principio del massimo sforzo.

Per creare una EventBridge regola per Audit Manager

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.

4. Nella pagina Definisci dettagli della regola, inserisci un nome e una descrizione per la regola.
5. Mantiei i valori predefiniti di per Bus di eventi e Tipo di regola, quindi scegli Avanti.
6. Nella pagina Crea modello di evento, per Event source, scegli AWS eventi o eventi EventBridge partner.
7. Come Metodo di creazione, sceglie Pattern personalizzato (editor JSON).
8. Nella sezione Modello di evento, scrivi un modello di evento in JSON e specifica i campi che desideri utilizzare per la corrispondenza.

   Per abbinare un evento Gestione audit, puoi utilizzare il seguente pattern semplice:

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Sostituisci *Evento* con uno dei seguenti valori supportati:

   a. Inserisci `Assessment Created` per ricevere notifiche quando viene creata una valutazione.
   b. Inserisci `Assessment Updated` per ricevere notifiche quando viene aggiornata una valutazione.
   c. Inserisci `Assessment Deleted` per ricevere notifiche quando viene eliminata una valutazione.
   d. Inserisci `Assessment ControlSet Delegation Created` per ricevere notifiche quando un set di controlli viene delegato per la revisione.
   e. Inserisci `Assessment ControlSet Reviewed` per ricevere notifiche quando un set di controlli di valutazione viene esaminato.
   f. Inserisci `Assessment Control Reviewed` per ricevere notifiche quando un controllo di valutazione viene esaminato.

   > **Tip**
   >
   > Se necessario, aggiungi altri campi al pattern del tuo evento. Per ulteriori informazioni sui campi disponibili, consulta Amazon EventBridge event patterns.

9. Seleziona Successivo.

10. Nella pagina Seleziona destinazioni, scegli la destinazione creata per questa regola, quindi configurare le eventuali altre opzioni richieste per quel tipo. Ad esempio, se scegli Amazon SNS, assicurati che il tuo argomento SNS sia configurato correttamente in modo da ricevere una notifica via e-mail o SMS.

    > **Tip**
    >
    > I campi visualizzati variano a seconda del servizio selezionato. Per ulteriori informazioni sugli obiettivi disponibili, consulta Target disponibili nella EventBridge console.

11. Per molti tipi di target, EventBridge sono necessarie le autorizzazioni per inviare eventi alla destinazione. In questi casi, EventBridge puoi creare il ruolo IAM necessario per l'esecuzione della regola.

    a. Per creare un ruolo IAM automaticamente, seleziona Crea un nuovo ruolo per questa risorsa specifica.

    b. Per utilizzare un ruolo IAM creato in precedenza, seleziona Utilizza un ruolo esistente.

12. (Facoltativo) Scegli Aggiungi destinazione per aggiungere un'altra destinazione per questa regola.
13. Seleziona Successivo.
14. (Facoltativo) Nella pagina Aggiungi tag, aggiungi tag alla chiave, quindi scegli Avanti.
15. Nella pagina Rivedi e crea, rivedi la configurazione della regola e fai in modo che soddisfi i requisiti di monitoraggio degli eventi.
16. Scegli Crea regola. La tua regola ora monitorerà gli eventi Gestione audit che vanno successivamente inviati alla destinazione specificata.

Registrazione delle chiamate AWS Audit Manager API con CloudTrail

Audit Manager è integrato con CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un Servizio AWS Audit Manager interno. CloudTrail acquisisce tutte le chiamate API per Audit Manager come eventi. Le chiamate acquisite includono le chiamate dalla console di Gestione audit e le chiamate di codice alle operazioni delle API Gestione audit.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Audit Manager. 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, è possibile determinare la richiesta effettuata a Audit Manager, 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.

Informazioni sull'Audit Manager in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Audit Manager, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi.

Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo Account AWS, compresi gli eventi per Audit Manager, 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 configurarne altri Servizi AWS 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 trail
- 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

Tutte le azioni di Audit Manager vengono registrate CloudTrail e documentate nell'AWS Audit Manager API Reference. Ad esempio, le chiamate alle operazioni `CreateControl`, `DeleteControl`, e `UpdateAssessmentFramework` API generano voci nei file di CloudTrail registro.

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.

- 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, vedete l'elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di log di Gestione audit

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'`CreateAssessment`azione.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
```

```
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

Comprensione della configurazione e dell'analisi delle vulnerabilità in AWS Audit Manager

La configurazione e i controlli IT sono una responsabilità condivisa tra voi AWS e voi, i nostri clienti. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Creazione di AWS Audit Manager risorse con AWS CloudFormation

AWS Audit Manager è integrato con AWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (ad esempio le valutazioni) e fornisce e AWS CloudFormation configura tali risorse per te.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse di Audit Manager in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più AWS account e regioni.

Audit Manager e AWS CloudFormation modelli

Per eseguire l'assegnazione e la configurazione delle risorse per Gestione audit e i servizi correlati, devi conoscere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri inserire nei tuoi AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

Audit Manager supporta la creazione di valutazioni in AWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le valutazioni, consulta Riferimento dei tipi di risorse AWS Audit Manager nella Guida per l'utente di AWS CloudFormation .

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Documentazione di riferimento delle API
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Utilizzo AWS Audit Manager con un AWS SDK

AWS i kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione popolari. Ogni SDK fornisce un'API, esempi di codice e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	questa documentazione specifica del servizio	Esempi di codice	
AWS SDK for C++	AWS SDK for C++ Riferimento API per Audit Manager	AWS SDK for C++ esempi di codice	
AWS SDK for Go	AWS SDK for Go Riferimento API per Audit Manager	AWS SDK for Go esempi di codice	
AWS SDK for Java	AWS SDK for Java 2.x Riferimento API per Audit Manager	AWS SDK for Java esempi di codice	
AWS SDK for JavaScript	AWS SDK for JavaScript Riferimento API per Audit Manager	AWS SDK for JavaScript esempi di codice	
AWS SDK for .NET	AWS SDK for .NET Riferimento API per Audit Manager	AWS SDK for .NET esempi di codice	
AWS SDK for PHP	AWS SDK for PHP Riferimento API per Audit Manager	AWS SDK for PHP esempi di codice	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto) Riferimento API per Audit Manager	AWS SDK for Python (Boto3) esempi di codice	
AWS SDK for Ruby	AWS SDK for Ruby Riferimento API per Audit Manager	AWS SDK for Ruby esempi di codice	

Per esempi specifici di questo servizio, consulta Esempi di codice per Audit Manager utilizzando gli AWS SDK.

> **Note**
>
> Gestione audit è disponibile nella versione botocore 1.19.32 e successive per AWS SDK for Python (Boto3). Prima di iniziare a utilizzare l'SDK, assicurati di utilizzare la versione botocore appropriata.

Disabilitazione AWS Audit Manager

È possibile disabilitare Gestione audit se non desideri più utilizzare il servizio. Quando disabiliti Gestione audit, hai anche la possibilità di eliminare tutti i tuoi dati.

Per impostazione predefinita, quando si disabilita Gestione audit, i dati non vengono eliminati. I dati relativi alle prove vengono conservati per due anni dal momento della loro creazione. Le altre risorse di Gestione audit (incluse valutazioni, controlli personalizzati e framework personalizzati) vengono conservate a tempo indeterminato e saranno disponibili se riabiliterai Gestione audit in futuro. Per ulteriori informazioni sulla conservazione dei dati, consulta la sezione Protezione dei dati in questa guida.

Se scegli di eliminare i tuoi dati, Gestione audit elimina tutti i dati relativi alle prove insieme a tutte le risorse di Gestione audit che hai creato (incluse valutazioni, controlli personalizzati e framework personalizzati). Tutti i dati vengono eliminati entro sette giorni dalla disattivazione di Gestione audit.

Argomenti

Procedura

È possibile disabilitare Audit Manager utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

> ⚠ Warning
>
> - Quando disabiliti Gestione audit, l'accesso viene revocato e il servizio non raccoglie più prove per le valutazioni esistenti. Se non riattivi Gestione audit, nessun contenuto del servizio sarà più disponibile.
> - L'eliminazione di tutti i dati è un'azione permanente. Se deciderai di riattivare Gestione audit in futuro, i tuoi dati non saranno recuperabili.

Audit Manager console

Per disabilitare Audit Manager sulla console Audit Manager

1. Dalla scheda Impostazioni generali, vai alla sezione Disabilita AWS Audit Manager.
2. Scegliere Disable (Disabilita Amazon Macie).
3. Nella finestra pop-up, rivedi l'attuale impostazione di conservazione dei dati.
    a. Per procedere con la selezione corrente, scegli Disabilita Gestione audit.
    b. Per modificare la selezione corrente, eseguire le fasi descritte di seguito:
        i. Scegli Annulla per tornare alla pagina delle impostazioni.
        ii. Per utilizzare l'impostazione di conservazione dei dati predefinita, disattiva Elimina tutti i dati. Questa selezione conserva i dati relativi alle prove per due anni dal momento della creazione e conserva altre risorse di Gestione audit a tempo indeterminato.
        iii. Per eliminare i dati, attiva Elimina tutti i dati.
        iv. Scegli Disabilita, quindi Disabilita Gestione audit per confermare la scelta.

AWS CLI

Prima di iniziare

Prima di disabilitare Gestione audit, puoi eseguire il comando update-settings per impostare la tua politica di conservazione dei dati preferita. Per impostazione predefinita, Gestione audit conserva i dati. Se desideri richiedere la cancellazione dei tuoi dati, utilizza il parametro `--deregistration-policy` con il valore `deleteResources` impostato su `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Per disabilitare Audit Manager in AWS CLI

Quando sei pronto a disabilitare Gestione audit, esegui il comando deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Prima di iniziare

Prima di disabilitare Audit Manager, puoi utilizzare l'operazione UpdateSettingsAPI per impostare la tua politica di conservazione dei dati preferita. Per impostazione predefinita, Gestione audit conserva i dati. Se desideri eliminare i tuoi dati, puoi utilizzare l'DeregistrationPolicyattributo per richiedere l'eliminazione dei tuoi dati.

Per disabilitare Audit Manager utilizzando l'API

Quando sei pronto a disabilitare Audit Manager, chiama l'DeregisterAccountoperazione.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nel Riferimento API Gestione audit. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Passaggi successivi

Se è necessario riattivare Audit Manager dopo averlo disabilitato, segui questi passaggi per ripristinare il servizio.

Per riattivare Gestione audit dopo averlo disabilitato

Vai alla home page del servizio Gestione audit e segui i passaggi per configurare Gestione audit come nuovo utente. Per ulteriori informazioni, consulta Configurazione AWS Audit Manager con le impostazioni consigliate.

Tip

- Se hai scelto di eliminare i tuoi dati quando hai disabilitato Gestione audit, devi attendere che i dati vengano eliminati prima di poter riattivare il servizio. A seconda della quantità di dati di cui disponi, questa operazione può richiedere fino a sette giorni. Tuttavia, puoi tentare liberamente di riattivare Gestione audit anche prima. In molti casi, i dati vengono eliminati in appena un'ora.
- Se hai scelto di non eliminare i tuoi dati quando hai disabilitato Gestione audit, le valutazioni esistenti sono passate a uno stato inattivo e di conseguenza hanno smesso di raccogliere prove. Per ricominciare a raccogliere prove per una valutazione preesistente, modifica la valutazione e scegli Salva senza apportare modifiche.

Risorse aggiuntive

- Per ulteriori informazioni sulla conservazione dei dati in Audit Manager, consulta la sezione Protezione dei dati in questa guida.

Cronologia dei documenti per la Guida AWS Audit Manager dell'utente

La tabella seguente descrive le modifiche importanti in ogni versione della Guida per l' AWS Audit Manager utente a partire dall'8 dicembre 2020.

Modifica	Descrizione	Data
Nuovo framework supportato: best practice di intelligenza artificiale AWS generativa v2	Un nuovo framework predefinito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta il framework AWS generativo per le migliori pratiche di intelligenza artificiale v2.	11 giugno 2024
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	10 giugno 2024
Utilizza i controlli comuni per semplificare il modo in cui esegui le valutazioni rispetto ai controlli aziendali	Quando crei un controllo personalizzato, ora puoi utilizzare i controlli comuni come fonte di prove. Ogni controllo comune è associato a un raggruppamento gestito di fonti di AWS dati pertinenti. Questi raggruppamenti predefiniti semplificano la raccolta delle prove eliminando la necessità di identificare quali AWS risorse devono essere valutate per un	6 giugno 2024

	determinato controllo. Per informazioni su come trovare controlli comuni e utilizzarli come fonti di evidenza, consulta la libreria Control.	
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	17 maggio 2024
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato la AWSAuditManagerAdministratorAccesspolitica. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	15 maggio 2024
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	15 maggio 2024
Support per chiamate AWS API aggiuntive	Ora puoi utilizzare chiamate AWS API aggiuntive come fonti di dati per i tuoi controlli personalizzati in Audit Manager. Per ulteriori informazioni, consulta Chiamate API supportate per origini dati di controllo personalizzate.	15 maggio 2024

Nuovo framework supportato: PCI DSS V4.0	Un nuovo framework precostruito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta PCI DSS V4.0.	19 dicembre 2023
Support per chiamate AWS API aggiuntive	Ora puoi utilizzare chiamate AWS API aggiuntive come fonti di dati per i tuoi controlli personalizzati in Audit Manager. Per ulteriori informazioni, consulta Chiamate API supportate per origini dati di controllo personalizzate.	7 dicembre 2023
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	6 dicembre 2023
Support per risultati di controllo AWS Security Hub consolidati	Audit Manager ora supporta i controlli consolidati in AWS Security Hub. Per ulteriori informazioni, consulta AWS Security Hub i controlli supportati da AWS Audit Manager.	16 novembre 2023
Integrazione con MetricStream	È ora possibile importare prove da Audit Manager in MetricStream. Per ulteriori informazioni, consulta Integrazione di prodotti GRC di terze parti.	14 novembre 2023

Nuovo framework supportato: best practice di intelligenza artificiale AWS generativa	Un nuovo framework predefinito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta il framework di best practice di IA generativa AWS v1.	8 novembre 2023
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	6 novembre 2023
Integrazione con Amazon EventBridge	Ora puoi monitorare gli eventi che si verificano AWS Audit Manager e utilizzarli come parte della tua architettura basata sugli eventi. Per ulteriori informazioni, consulta Monitoraggio AWS Audit Manager con Amazon EventBridge.	18 agosto 2023

Supporto per le valutazioni del rischio e nuove opzioni di prove manuali	È ora possibile utilizzare il flusso di lavoro personalizzato per la creazione di controlli a supporto delle valutazioni del rischio. Ora un controllo può rappresentare una domanda di valutazione del rischio ed è possibile fornire una risposta caricando un file o inserendo del testo come prova manuale. Per ulteriori informazioni, consulta Creare un controllo personalizzato e Aggiungere prove manuali.	12 giugno 2023
Supporto per le esportazioni in formato CSV	È ora possibile esportare i risultati della ricerca di Evidence Finder in formato CSV. Per ulteriori informazioni, consulta Esportare i risultati della ricerca.	9 giugno 2023
Nuovo framework supportato: Australian Cyber Security Centre (ACSC) Information Security Manual	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni, consulta l'Australian Cyber Security Centre (ACSC) Information Security Manual.	24 marzo 2023

Report di valutazione migliorati	Abbiamo apportato miglioramenti al formato e ai contenuti dei report di valutazione di Gestione audit. Per ulteriori informazioni su come navigare e comprendere i report di valutazione, consulta Report di valutazione.	23 marzo 2023
Supporto per le chiamate API restituite	AWS Audit Manager ora supporta le chiamate API impaginate come fonte di dati per la raccolta di prove. Per ulteriori informazioni, consulta Chiamate API restituite.	8 marzo 2023
Nuovo framework supportato: HIPAA Final Omnibus Security Rule 2013	Un nuovo framework predefinito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta HIPAA Final Omnibus Security Rule 2013. Per fini di differenziazione, il precedente framework HIPAA (denominato HIPAA nella libreria dei framework) è ora denominato HIPAA Security Rule 2003.	8 marzo 2023
Support per chiamate AWS API aggiuntive	Ora puoi utilizzare altre nove chiamate AWS API come fonte di dati per i controlli personalizzati in Audit Manager. Per ulteriori informazioni, consulta Chiamate API supportate per origini dati di controllo personalizzate.	3 marzo 2023

Guida aggiornata per l'allineamento alle best practice IAM	Guida aggiornata per l'allineamento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	6 gennaio 2023
Nuova impostazione di conservazione dei dati	Ora puoi decidere se eliminare tutti i tuoi dati quando disabilit i Gestione audit. Per ulteriori informazioni, consulta Disabilitazione AWS Audit Manager ed Eliminazione dei dati di Gestione audit.	6 gennaio 2023
Supporto per Evidence Finder	È ora possibile utilizzare Evidence Finder per eseguire query di ricerca sui dati delle prove. Per ulteriori informazioni, consulta Evidence Finder.	18 novembre 2022
Nuovo framework supportato: Australian Cyber Security Centre (ACSC) Essential Eight	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni consulta Australian Cyber Security Centre (ACSC) Essential Eight.	24 agosto 2022
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	7 luglio 2022

Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	20 maggio 2022
Nuovo framework supportato: Canadian Centre for Cyber Security Medium Cloud Control Profile	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni, consulta Canadian Centre for Cyber Security Medium Cloud Control Profile.	6 maggio 2022
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato la AWSAuditManagerAdministratorAccesspolitica. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	29 aprile 2022
Support per regole AWS Config gestite aggiuntive	È ora possibile utilizzare altre 91 regole AWS Config gestite come origine dati per i controlli personalizzati in Audit Manager. Per ulteriori informazioni, vedere Utilizzo di regole AWS Config gestite con AWS Audit Manager.	27 aprile 2022

Support per regole AWS Config personalizzate	È ora possibile utilizzare le regole AWS Config personalizzate come fonte di dati per i controlli personalizzati in Audit Manager. Per ulteriori informazioni, vedere Utilizzo di regole AWS Config personalizzate con AWS Audit Manager.	27 aprile 2022
Nuovo framework supportato: ISO/IEC 27001:2013 Annex A	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni, consulta ISO/IEC 27001:2013 Annex A.	7 aprile 2022
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy. Per ulteriori informazioni, consulta Policy gestite da AWS per AWS Audit Manager.	16 marzo 2022
Nuovi framework supportati: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4	Sono ora disponibili due nuovi framework predefiniti AWS Audit Manager: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 e CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 e 2. Per ulteriori informazioni, consulta CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 marzo 2022

Nuovo framework supportato: CIS Controls v8 IG1	Un nuovo framework precostruito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta CIS Controls v8 IG1.	2 marzo 2022
AWS Audit Manager pannello di controllo	È ora possibile utilizzare la dashboard di Gestione audit per monitorare le valutazioni attive e identificare rapidamente le prove non conformi. Per ulteriori informazioni, consulta Utilizzo della dashboard di Gestione audit.	18 novembre 2021
Condivisione di un framework personalizzato	Ora puoi condividere i tuoi framework Audit Manager personalizzati con un altro Account AWS utente o replicarli in un altro con il tuo Regione AWS account. Per ulteriori informazioni, consulta Condivisione di un framework personalizzato.	22 ottobre 2021
Nuovi esempi di controlli AWS Audit Manager	Ora puoi esaminare esempi di controlli e scoprire come Audit Manager aiuta a rendere il tuo AWS ambiente in linea con i loro requisiti. Per ulteriori informazioni, consulta Esempi di AWS Audit Manager controlli.	21 settembre 2021

Nuovo framework supportato: Gramm-Leach-Bliley Act (GLBA)	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni, consulta Gramm-Leach-Bliley Act (GLBA).	2 settembre 2021
Nuovo capitolo sulla risoluzione dei problemi	È ora disponibile un nuovo capitolo sulla risoluzione dei problemi. Per ulteriori informazioni, vedere Risoluzione dei problemi in AWS Audit Manager.	23 agosto 2021
Nuovo capitolo e tutorial sulla delega	Abbiamo ampliato la nostra documentazione sulla delega in un nuovo capitolo. Per ulteriori informazioni, vedere Deleghe in AWS Audit Manager. Abbiamo anche aggiunto un nuovo tutorial rivolto ai delegati che stanno esaminando un set di controlli per la prima volta. AWS Audit Manager Per ulteriori informazioni, consulta Tutorial per i delegati: revisione di un set di controlli.	25 giugno 2021
Nuovo framework supportato: NIST SP 800-171 Rev. 2	Un nuovo framework predefinito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta NIST SP 800-171 Rev. 2.	17 giugno 2021

Report di valutazione migliorati	Abbiamo apportato miglioramenti al formato e al contenuto dei rapporti di AWS Audit Manager valutazione. Per ulteriori informazioni su come navigare e comprendere i nuovi report di valutazione, consulta Report di valutazione.	8 giugno 2021
Nuova pagina delle politiche AWS gestite	AWS Audit Manager ha iniziato a tenere traccia delle modifiche relative alle politiche gestite. Per ulteriori informazioni, consulta la sezione Policy gestite AWS per AWS Audit Manager.	6 maggio 2021
Nuovo framework supportato: NIST Cybersecurity Framework versione 1.1	Un nuovo framework predefinito è ora disponibile in AWS Audit Manager. Per ulteriori informazioni, consulta NIST Cybersecurity Framework versione 1.1.	5 maggio 2021
Nuovo framework supportato: AWS Well-Architected	Un nuovo framework precostruito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta AWS Well-Architected.	5 maggio 2021
Nuovo framework supportato: AWS Foundational Security Best Practices	Un nuovo framework predefinito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta AWS Foundational Security Best Practices.	5 maggio 2021

Nuovo framework supportato: GxP EU Annex 11	Un nuovo framework precostruito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta GxP EU Annex 11.	28 Aprile 2021
Nuovo framework supportato: NIST 800-53 (Rev. 5) Low-Moderate-High	Un nuovo framework precostruito è ora disponibile in. AWS Audit Manager Per ulteriori informazioni, consulta NIST 800-53 (Rev. 5) Low-Moderate-High.	25 marzo 2021
Nuovi framework supportati: CIS Benchmark per CIS Foundations Benchmark v1.3 AWS Audit Manager	Sono ora disponibili due nuovi framework predefiniti AWS Audit Manager: CIS Benchmark for CIS Foundations Benchmark v1.3.0, Level 1 e CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 e 2. AWS Audit Manager Per ulteriori informazioni, consulta CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 marzo 2021
Versione iniziale	Versione iniziale AWS Audit Manager della Guida per l'utente e dell'API Reference.	8 dicembre 2020

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.