



Guida per l'utente

AWS Audit Manager



AWS Audit Manager: Guida per l'utente

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

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

Table of Contents

Cos'è AWS Audit Manager?	1
Caratteristiche di AWS Audit Manager	1
Prezzi di AWS Audit Manager	2
È la prima volta che utilizzi Audit Manager?	3
Altre risorse AWS Audit Manager	3
Concetti e terminologia	3
A	3
C	6
D	9
E	12
F	15
R	16
S	17
Raccolta di prove	18
Frequenza di raccolta delle prove	19
Esempi di controlli	20
Controlli automatici (Security Hub)	21
Controlli automatici (AWS Config)	23
Controlli automatici (chiamate API)	25
Controlli automatici (CloudTrail)	27
Controlli manuali	29
Controlli con origini dati miste	31
Integrazioni Servizio AWS	33
Integrazioni con GRC di terze parti	35
Comprensione delle integrazioni di terze parti	35
Prodotti GRC di terze parti supportati	36
Utilizzo di Audit Manager con un SDK AWS	38
Configurazione	40
Prerequisiti	40
Iscriviti per un Account AWS	40
Crea un utente con accesso amministrativo	41
Aggiungi le autorizzazioni richieste	42
Abilitazione di Audit Manager	43
Raccomandazioni	47

Funzionalità consigliate	48
Integrazioni consigliate	48
Cosa devo fare dopo?	54
Inizia a usare	54
Aggiornare le impostazioni di Maven	54
Nozioni di base	55
Tutorial Audit Manager	55
Tutorial per i proprietari degli audit: creazione di una valutazione	56
Fase 1: specificare i dettagli della valutazione	57
Fase 2: specificare gli account pertinenti	58
Fase 3: specificare i servizi nell'ambito di applicazione	58
Fase 4: specificare i proprietari dell'audit	59
Passaggio 5: revisione e creazione	59
A questo punto come si può procedere?	60
Tutorial per delegati: revisione di un set di controlli	60
Fase 1: accesso alle notifiche	61
Fase 2: esaminare un set di controlli e le prove	62
Fase 3: carica le prove manuali	63
Fase 4: aggiungi un commento	64
Fase 5: aggiorna lo stato di controllo	65
Fase 6. Restituisci il set di controlli revisionato al proprietario dell'audit	65
A questo punto come si può procedere?	66
Utilizzo del pannello di controllo	67
Concetti e terminologia del pannello di controllo	68
Elementi del pannello di controllo	71
Filtro di valutazione	71
Snapshot giornaliero	72
Controlli con prove non conformi raggruppati per dominio di controllo	73
Cosa devo fare dopo?	75
Risoluzione dei problemi	75
Valutazioni	76
Creazione di una valutazione	77
Fase 1: specificare i dettagli della valutazione	77
Fase 2: specificare gli account pertinenti	79
Fase 3: specificare i servizi nell'ambito di applicazione	80
Fase 4: specificare i proprietari dell'audit	81

Passaggio 5: revisione e creazione	81
Cosa posso fare dopo?	82
Accedere a una valutazione	82
Modifica di una valutazione	83
Fase 1: modificare i dettagli della valutazione	84
Fase 2: Modifica gli account nell'ambito	84
Fase 3: modifica i servizi nell'ambito	85
Fase 4: modificare i proprietari dell'audit	86
Fase 5: revisione e salvataggio	86
Revisione di una valutazione	87
Dettagli della valutazione	87
Scheda Controlli	88
Scheda di selezione del report di valutazione	89
Account AWS linguetta	90
Servizi AWS linguetta	90
Scheda titolari audit	91
Scheda Tag	92
Scheda Changelog	92
Revisione dei controlli di valutazione	93
Dettagli del controllo	93
Stato del controllo	94
Scheda Cartelle delle prove	94
Scheda Origine dati	95
Scheda Commenti	96
Scheda Changelog	96
Esame delle prove	97
Revisione delle cartelle delle prove	98
Revisione delle prove individuali	100
Aggiunta di prove manuali	102
Come aggiungere prove manuali	103
Formati file supportati	112
Generazione di un report di valutazione	112
Aggiungere prove	113
Rimozione delle prove	114
Generazione di un report	115
Cosa posso fare dopo?	115

Modifica dello stato di una valutazione	116
Eliminazione di una valutazione	118
Deleghe	121
Per i proprietari dell'audit	121
Delega di un set di controlli	122
Accesso alle deleghe	124
Eliminazione delle deleghe	125
Per i delegati	126
Visualizzazione delle notifiche	126
Revisione dei controlli e delle prove	127
Aggiungere commenti	129
Contrassegnare un controllo come revisionato	129
Invio di un set di controlli al proprietario dell'audit	130
Report di valutazione	131
Struttura della cartella	131
Come navigare in un report	131
Sezioni del report	132
Frontespizio	133
Pagina di panoramica	133
Pagina del sommario	134
Pagina di controllo	134
Pagina di riepilogo delle prove	136
Pagina dei dettagli delle prove	137
Verifica dell'integrità del report	137
Risoluzione dei problemi	137
Evidence finder	138
Comprendere come funziona evidence finder con CloudTrail Lake	138
Attivazione di evidence finder	139
Risoluzione dei problemi evidence finder	139
Ricerca le prove	139
Esecuzione di una query di ricerca	140
Interruzione di una query di ricerca	142
Modificare i filtri di ricerca	142
Visualizzare i risultati in evidence finder	144
Visualizzazione dei risultati raggruppati	144
Visualizzazione dei risultati	145

Filtro e opzioni di raggruppamento	152
Riferimento al filtro	152
Riferimento di raggruppamento	158
Casi d'uso di esempio	158
Caso d'uso 1: trovare prove non conformi e organizzare le delegazioni	159
Caso d'uso 2: Identifica le prove conformi	159
Caso d'uso 3: Esegui una rapida anteprima delle risorse relative alle prove	160
Centro di download	162
Navigazione nel centro di download	162
Scaricamento di un file	163
Eliminazione di un file	164
Libreria Framework	165
Accesso a un framework	166
Visualizzazione dei dettagli del framework	167
Creazione di un framework personalizzato	170
Crea nuovo	171
Personalizza l'esistente	173
Modifica di un framework personalizzato	176
Fase 1: specificare i dettagli del framework	176
Fase 2: modificare i controlli	177
Fase 3. Revisione e aggiornamento	178
Eliminazione di un framework personalizzato	178
Condivisione di un framework personalizzato	179
Concetti e terminologia di condivisione	181
Invio di una richiesta di condivisione	189
Risposta alla richiesta di condivisione	195
Eliminazione di una richiesta di condivisione	200
Framework supportati	200
ACSC Essential Eight	201
ISM ACSC	204
Framework di esempio AWS Audit Manager	206
Guardrail AWS Control Tower	208
Best practice di IA generativa AWSper Amazon Bedrock	210
AWS License Manager	218
AWS Foundational Security Best Practices	220
Best practice operative AWS	223

AWS Well-Architected	225
CCCS Medium Cloud Control Profile	227
CIS AWSFoundations Benchmark v.1.2	230
CIS AWSFoundations Benchmark v.1.3	240
CIS AWSFoundations Benchmark v.1.4	244
Controlli CIS v7.1 IG1	248
CIS Controls v8 IG1	251
FedRAMP Moderate Baseline	254
Regolamento generale sulla protezione dei dati (GDPR)	257
Gramm-Leach-Bliley Act	283
GxP 21 CFR parte 11	285
GxP UE Allegato 11	288
Norma di sicurezza HIPAA 2003	291
Norma di sicurezza Omnibus finale HIPAA 2013	294
ISO/IEC 27001:2013	297
NIST 800-53 (Rev. 5)	300
NIST CSF v1.1	303
NIST SP 800-171 (Rev. 2)	306
PCI DSS v3.2.1	309
PCI DSS v4	312
SOC 2	316
Libreria di controllo	320
Accedere a un controllo	320
Visualizzazione dei dettagli di controllo	322
Creazione di un controllo personalizzato	325
Crea nuovo	327
Personalizza l'esistente	330
Modifica di un controllo personalizzato	334
Fase 1: modifica dei dettagli di controllo	334
Fase 2: modifica origini dati	335
Fase 3: modifica del piano di azione	336
Fase 4: Revisione e aggiornamento	336
Eliminazione di un controllo personalizzato	337
Modifica della frequenza di raccolta delle prove	338
Istantanee di configurazione dalle chiamate API	339
Controlli di conformità da AWS Config	340

Controlli di conformità da Security Hub	341
Registri delle attività degli utenti da AWS CloudTrail	342
Controllo delle origini dati	342
Origini dati automatici	343
AWS Config	346
AWS Security Hub	361
AWS Chiamate API	409
AWS CloudTrail	420
Impostazioni	422
Impostazioni generali	422
Autorizzazioni	423
Crittografia dei dati	423
Amministratore delegato (facoltativo)	425
AWS Config (facoltativo)	433
Security Hub (facoltativo)	433
Disabilita AWS Audit Manager	433
Impostazioni di valutazione	436
Proprietari di audit predefiniti (opzionale)	436
Destinazione del rapporto di valutazione (opzionale)	437
Notifiche (facoltativo)	440
Impostazioni di evidence finder	442
Strumento evidence finder (opzionale)	442
Destinazione di esportazione (facoltativo)	448
Notifiche	452
Prerequisiti	452
Configurazione delle notifiche in AWS Audit Manager	452
Risoluzione dei problemi	453
Risoluzione dei problemi	454
Valutazioni e raccolta di prove	454
Ho creato una valutazione ma non riesco ancora a visualizzare alcuna prova	455
La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub	456
Ho disabilitato un controllo di sicurezza in Security Hub. Audit Manager raccoglie le prove dei controlli di conformità per quel controllo di sicurezza?	458
Ho impostato lo stato di un risultato su Suppressed Security Hub. Audit Manager raccoglie prove di verifica della conformità relative a tale risultato?	458

La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Config ..	458
La mia valutazione non sta raccogliendo prove dell'attività degli utenti da AWS CloudTrail ..	461
La mia valutazione non sta raccogliendo prove dei dati di configurazione per una chiamata AWS API	461
La mia valutazione non sta raccogliendo prove da un altro Servizio AWS	462
Le mie prove vengono generate a intervalli diversi e non sono sicuro della frequenza con cui vengono raccolte	462
Cosa succede se rimuovo un account in ambito dalla mia organizzazione?	464
Non riesco a modificare i servizi in ambito per la mia valutazione	464
Qual è la differenza tra un servizio in ambito e un tipo di origine dati?	464
La creazione della mia valutazione non è riuscita	466
Ho disabilitato e poi riabilitato Audit Manager e ora le mie valutazioni preesistenti non raccolgono più prove	466
Report di valutazione	466
Il report di valutazione non è stato generato	467
Ho seguito l'elenco di controllo sopra riportato e il mio report di valutazione non è ancora stato generato	468
Ricevo un errore di accesso negato quando provo a generare un report	468
Non riesco a decomprimere il report di valutazione	469
Quando scelgo il nome di una prova in un report, non vengo reindirizzato ai dettagli della prova	470
La generazione del mio report di valutazione è bloccata nello stato In corso e non so come ciò influisca sulla mia fatturazione	470
Consulta anche	470
Controlli e set di controlli	471
Non riesco a vedere alcun controllo o set di controlli nella mia valutazione	471
Non riesco a caricare prove manuali su un controllo	472
Devo utilizzare più AWS Config regole come fonte di dati per un singolo controllo	472
L'opzione delle regole personalizzate non è disponibile per la mia origine dati	472
L'elenco a discesa delle regole personalizzate è vuoto	473
Non riesco a vedere la regola personalizzata che voglio usare	473
Non riesco a vedere la regola gestita che voglio usare	474
Voglio condividere un framework personalizzato, ma include controlli che utilizzano regole AWS Config personalizzate come origine dati	477
Cosa succede quando una regola personalizzata viene aggiornata in AWS Config?	478
Dashboard	479

Non ci sono dati nella mia dashboard	480
L'opzione di download in formato CSV non è disponibile	480
Non vedo il file scaricato quando cerco di scaricare un file CSV	480
Nella dashboard non è presente un controllo o un dominio di controllo specifico	480
Lo snapshot quotidiano mostra ogni giorno quantità diverse di prove. È normale che sia così?	481
Amministratori delegati e AWS Organizations	481
Non riesco a configurare Audit Manager con il mio account di amministratore delegato	482
Quando creo una valutazione, non riesco a visualizzare gli account della mia organizzazione in Account in ambito	482
Ricevo un errore di accesso negato quando provo a generare un report di valutazione utilizzando il mio account di amministratore delegato	483
Cosa succede in Audit Manager se scollego un account membro dalla mia organizzazione?	484
Cosa succede se ricollego un account membro alla mia organizzazione?	484
Cosa succede se eseguo la migrazione di un account membro da un'organizzazione all'altra?	484
Evidence Finder	484
Non riesco ad abilitare Evidence Finder	485
Ho abilitato Evidence Finder, ma non vedo prove precedenti nei risultati di ricerca	486
Non riesco a disabilitare Evidence Finder	486
La mia query di ricerca non riesce	487
Non riesco a generare più report di valutazione dai miei risultati di ricerca	489
Non posso includere prove specifiche dai miei risultati di ricerca	490
Non tutti i risultati del mio Evidence Finder sono inclusi nel report di valutazione	490
Desidero generare un report di valutazione dai risultati della mia ricerca, ma la mia istruzione di query non riesce a essere eseguita.	491
Altre risorse	494
La mia esportazione in formato CSV non è riuscita	494
Non posso esportare prove specifiche dai miei risultati di ricerca	496
Non riesco a esportare più file CSV contemporaneamente	496
Condivisione del framework	497
Lo stato della richiesta di condivisione inviata viene visualizzato come Non riuscito	497
La mia richiesta di condivisione è contrassegnata da un punto blu. Che cosa significa?	498
Il mio framework condiviso ha controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?	501

Ho aggiornato una regola personalizzata utilizzata in un framework condiviso. Devo fare qualcosa?	501
Notifiche	503
Ho specificato un argomento di Amazon SNS in Audit Manager, ma non ho ricevuto alcuna notifica	503
Ho specificato un argomento FIFO, ma non ricevo notifiche nell'ordine previsto	504
Autorizzazioni e accessi	504
Ho seguito la procedura di configurazione di Audit Manager, ma non dispongo di privilegi IAM sufficienti	504
Ho indicato qualcuno come proprietario dell'audit, ma non ha ancora pieno accesso alla valutazione. Perché?	505
Non riesco a eseguire un'operazione in Audit Manager	505
Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Audit Manager	505
Consulta anche	470
Quote	507
Quote predefinite di Audit Manager	507
Gestione delle proprie quote	508
Sicurezza	510
Protezione dei dati	511
Eliminazione dei dati di Audit Manager	512
Crittografia a riposo	513
Crittografia in transito	514
Gestione delle chiavi	514
Gestione dell'identità e degli accessi	515
Destinatari	515
Autenticazione con identità	516
Gestione dell'accesso con policy	520
Come AWS Audit Manager funziona con IAM	522
Esempi di policy basate su identità	532
Prevenzione del confused deputy tra servizi	552
AWS politiche gestite	553
Risoluzione dei problemi	583
Uso di ruoli collegati ai servizi	585
Convalida della conformità	598
Resilienza	600

Sicurezza dell'infrastruttura	600
Endpoint VPC (AWS PrivateLink)	601
Considerazioni sugli endpoint AWS Audit Manager VPC	601
Creazione di un endpoint VPC interfaccia per l' AWS Audit Manager	601
Creazione di una policy per gli endpoint VPC per AWS Audit Manager	602
Registrazione di log e monitoraggio	602
Monitoraggio con Amazon EventBridge	603
CloudTrail registri	607
Configurazione e vulnerabilità	610
Assegnazione di tag alle risorse	611
Risorse supportate	611
Limitazioni applicate ai tag	611
Gestione dei tag in Audit Manager	612
Risorse AWS CloudFormation	613
Audit Manager e modelli AWS CloudFormation	613
Ulteriori informazioni su AWS CloudFormation	613
Cronologia dei documenti	614
Glossario per AWS	626
.....	dcxxvii

Cos'è AWS Audit Manager?

Benvenuto nella Guida per l'utente di AWS Audit Manager.

AWS Audit Manager aiuta a verificare continuamente l'utilizzo di AWS per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore. Audit Manager 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, Audit Manager 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.

Audit Manager 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, Audit Manager esegue automaticamente le valutazioni delle risorse. Le valutazioni raccolgono dati sia per Account AWS e i servizi definiti 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 Audit Manager per raccogliere le prove, è possibile interrompere la raccolta delle prove. Per farlo, occorre modificare lo stato della valutazione in Inattiva.

Caratteristiche di Audit Manager

Con AWS Audit Manager puoi eseguire le seguenti operazioni:

- 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 verificare il tuo utilizzo di Servizio AWS.
- Carica e gestisci le prove da ambienti ibridi o multicloud: oltre alle prove che Audit Manager 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. Comprendono CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA, SOC2, GxP e le best practice operative AWS.
- Monitora le valutazioni attive: utilizza la [dashboard](#) di Audit Manager 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 funzione di [ricerca delle prove](#) 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 i tuoi controlli da zero](#) o [personalizza un controllo esistente per soddisfare le tue esigenze](#). 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.
- Personalizza i framework: [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 altri Account AWS o replicali in un altro Regione AWS all'interno del 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 normative di conformità. Tuttavia, non esegue valutazioni di conformità. Pertanto, le prove raccolte tramite AWS Audit Manager potrebbero non includere tutte le informazioni sull'utilizzo di AWS necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Prezzi di Audit Manager

Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Audit Manager](#).

È la prima volta che utilizzi Audit Manager?

Se utilizzi Audit Manager per la prima volta, ti consigliamo di iniziare dalle seguenti pagine:

1. [AWS Audit Manager concetti e terminologia](#): scopri i concetti e i termini chiave utilizzati in Audit Manager, come valutazioni, framework e controlli.
2. [Come AWS Audit Manager raccoglie le prove](#): scopri come Audit Manager raccoglie le prove per una valutazione delle risorse.
3. [Configurazione](#): scopri i requisiti di configurazione di Audit Manager.
4. [Guida introduttiva](#): segui un tutorial per creare la tua prima valutazione con Audit Manager.
5. [AWS Audit Manager Riferimento API](#): acquisisci familiarità con le azioni e i tipi di dati dell'API Audit Manager.

Altre risorse Audit Manager

Le risorse seguenti forniscono ulteriori informazioni su Audit Manager.

- [Raccogli prove e gestisci i dati di audit utilizzando AWS Audit Manager](#)
- [Configura manualmente una valutazione personalizzata di Audit Manager](#) da AWS Workshops
- [Integra con il modello a tre righe \(Parte 2\): trasforma i pacchetti di conformità AWS Config in AWS Audit Manager valutazioni](#) tratte dal blog AWS Management & Governance

concetti e terminologia AWS Audit Manager

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

A

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Valutazione

È possibile utilizzare una valutazione di Audit Manager 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. A seconda delle esigenze aziendali, è possibile 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. Per contro, i framework personalizzati contengono controlli che è possibile personalizzare e raggruppare in base ai requisiti di audit interno. Utilizzando un framework come punto di partenza, è possibile creare una valutazione che specifichi gli Account AWS e i servizi che si desidera includere nell'ambito dell'audit.

Quando si crea una valutazione, Audit Manager inizia automaticamente a valutare le risorse dell'utente negli Account AWS nei servizi in 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 effettuare 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 [Valutazioni in AWS Audit Manager](#).

Report di valutazione

Un report di valutazione è un documento definitivo generato da una valutazione di Audit Manager. 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 Audit Manager 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 [Generazione di un report di valutazione](#).

Destinazione del report di valutazione

La destinazione dei report di valutazione è il bucket S3 predefinito in cui Audit Manager salva i report di valutazione. Per ulteriori informazioni, consulta [Destinazione del rapporto di valutazione \(opzionale\)](#).

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 Audit Manager, il proprietario dell'audit è un utente o un ruolo che gestisce una valutazione e le relative risorse. Le responsabilità di questo Audit Manager includono la creazione di valutazioni, la revisione delle prove e la generazione di report di valutazione. Audit Manager 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 Audit Manager di un proprietario dell'audit, non solo i professionisti GRC. Ad esempio, potresti scegliere di far configurare e gestire le valutazioni di Audit Manager 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 Audit Manager dipende molto dall'organizzazione. Dipende anche da come si strutturano le operazioni di sicurezza e dalle specifiche dell'audit. In Audit Manager, 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 Audit Manager, 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, Audit Manager garantisce il pieno controllo su tutte le specifiche di una valutazione individuale. Per ulteriori informazioni, consulta [Policy consigliate per i profili utente in AWS Audit Manager](#).

C

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Changelog

Per ogni controllo in una valutazione, Audit Manager acquisisce i changelog per tenere 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 su quali attività degli utenti vengono registrate nei changelog, consulta [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.

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 di sicurezza 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 Audit Manager, 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 Audit Manager. È anche possibile aggiungere manualmente prove a qualsiasi controllo. Ogni prova diventa un documento che aiuta a dimostrare la conformità ai requisiti del controllo.

Esistono due tipi di controlli in Audit Manager:

- **Controlli standard:** si tratta di controlli predefiniti associati a un framework specifico in Audit Manager. Utilizza i controlli ordinari come aiuto alla preparazione degli audit per vari standard e regolamenti di conformità.
- **Controlli personalizzati:** si tratta di controlli personalizzati che definisci come utente Audit Manager. Utilizza i controlli personalizzati come aiuto per soddisfare requisiti di conformità specifici di audit interni o le valutazioni del rischio del fornitore.

Per ulteriori informazioni, consulta [Esempi di AWS Audit Managercontrolli](#). Per istruzioni su come creare e gestire i controlli, consulta [Libreria di controllo](#).

Domini 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 di Audit Manager](#). Audit Manager 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.

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.

Audit Manager classifica i controlli nei seguenti domini di controllo.

Nome del dominio di controllo	Descrizione di cosa regolano questi controlli
Continuità aziendale e pianificazione delle emergenze	Come stabilire processi che proteggano le operazioni aziendali critiche dagli effetti di gravi interruzioni di sistema e di rete.
Gestione delle modifiche	Come testare, approvare, implementare e documentare le modifiche alla propria infrastruttura cloud.
Sicurezza e privacy dei dati	Come proteggere la privacy, la disponibilità e l'integrità dei dati.
Sviluppo e gestione della configurazione	Come mantenere l'infrastruttura cloud nello stato desiderato e coerente.
Governance e supervisione	Come allineare l'uso del cloud computing agli obblighi legali, normativi ed etici.
Identity and Access Management	Come garantire che gli utenti giusti abbiano l'accesso appropriato alle risorse tecnologiche.
Gestione degli incidenti	Come stabilire responsabilità e procedure che garantiscano una risposta rapida ed efficace agli incidenti di sicurezza.
Registrazione di log e monitoraggio	Come esaminare l'attività degli utenti alla ricerca di indizi che dimostrino il tentativo di esecuzione o l'esecuzione di attività non autorizzate.
Gestione di rete	Come amministrare e gestire la rete di dati utilizzando un sistema di gestione di rete.
Gestione del personale	Come valutare e gestire i rischi per la sicurezza del personale a livello organizzativo.

Nome del dominio di controllo	Descrizione di cosa regolano questi controlli
Sicurezza fisica	Come rilevare e prevenire i problemi di sicurezza fisica nelle proprie strutture.
Gestione del rischio	Come valutare i rischi e le perdite potenziali e come ridurre o eliminare tali minacce.
Gestione della catena di fornitura	Come identificare, valutare e mitigare i rischi associati ai prodotti, ai fornitori e alle catene di fornitura IT.
Gestione dei dispositivi utente	Come ridurre il rischio che l'hardware IT dei dipendenti venga perso, danneggiato o compromesso.
Gestione delle vulnerabilità	Come definire, valutare e porre rimedio a tutte le vulnerabilità note delle risorse all'interno della propria infrastruttura cloud.

D

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Origine dati

Audit Manager utilizza un'origine dati per raccogliere le prove per un controllo. La terminologia seguente descrive cos'è e come funziona un'origine dati.

- Un tipo di origine dati definisce da dove Audit Manager raccolga le prove per un controllo. Se carichi le tue prove, il tipo di origine dati è Manuale. Se Audit Manager raccoglie le prove per tuo conto, il tipo di origine dati è uno dei seguenti: AWS Security Hub, AWS Config, AWS CloudTrail o chiamate API AWS. API Audit Manager fa riferimento a un tipo di origine dati come [SourceType](#) (singolare) o [ControlSources](#) (plurale).
- Una mappatura è una parola chiave specifica che si riferisce a un tipo di origine dati. Ad esempio, potrebbe essere il nome di un evento CloudTrail o un nome AWS Config. [API Audit Manager fa riferimento a questo come SourceKeyword \(singolare\) o ControlMappingSources \(plurale\)](#).
- Un nome di origine dati è un nome assegnato a un'origine dati. In altre parole, il nome di un'origine dati etichetta la combinazione di un tipo di origine dati e di una mappatura. Per i

controlli ordinari, Audit Manager fornisce un nome di origine dati predefinito (ad esempio Origine dati 1 e Origine dati 2). Per i controlli personalizzati, puoi fornire il nome della tua origine dati. Questo potrebbe aiutarti a distinguere tra più mappature che rientrano nello stesso tipo di origine dati. API Audit Manager 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 origine dati (ad esempio AWS Config e Security Hub). Un altro controllo potrebbe avere AWS Config come unico tipo di origine dati, con più regole AWS Config 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'istantanea dello stato di sicurezza delle tue risorse. Audit Manager 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.	1.1 - Avoid the use of the "root" account
AWS Config	Utilizza questo tipo di origine dati per acquisire un'istantanea dello stato di sicurezza delle tue risorse. Audit Manager utilizza il nome di una regola AWS Config come parola chiave di mappatura ed esegue il report del risultato di tale	EC2_INSTANCE_MANAGED_BY_SSM

Tipo di origine dati	Descrizione	Esempio di mappatura
	regola direttamente da Security AWS Config.	
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 evento CloudTrail come parola chiave di mappatura e raccoglie l'attività utente correlata dai tuoi log di CloudTrail.	CreateAccessKey
AWSChiamate API	Utilizza questo tipo di origine dati per scattare un'istantanea della configurazione delle tue risorse tramite una chiamata API a una determinata Servizio AWS. Audit Manager utilizza il nome della chiamata API come parola chiave di mappatura e raccoglie la risposta API.	ec2_DescribeSecurityGroups

L'immagine seguente mostra esempi di diverse origini dati visualizzate nella console Audit Manager.

Data sources (4)				
Data source name	Data source type	Mapping	Frequency	
Data source 1	AWS API calls	iam_ListRoles	Daily	
Data source 2	AWS API calls	iam_ListGroups	Daily	
Data source 3	AWS API calls	iam_ListUsers	Daily	
Data source 4	AWS API calls	iam_ListPolicies	Daily	

Note

Sebbene alcuni tipi di origine dati siano Servizi AWS, un tipo di origine dati è diverso da un servizio in ambito. Per ulteriori informazioni, consulta [Qual è la differenza tra un servizio in ambito e un tipo di origine dati?](#) nella sezione Risoluzione dei problemi di questa guida.

Delegato

Un delegato è un utente AWS Audit Manager 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 [Deleghe in AWS Audit Manager](#).

E

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [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 Audit Manager: prove automatiche e prove manuali.

- Prove automatiche: si tratta delle prove che Audit Manager raccoglie automaticamente. Sono incluse le seguenti tre categorie di prove automatiche:
 - Controllo di conformità: il risultato di un controllo di conformità viene acquisito da AWS Security Hub, AWS Config da entrambi. Esempi di controlli di conformità includono un risultato del controllo di sicurezza di Security Hub per un controllo PCI DSS e una valutazione delle regole AWS Config per un controllo HIPAA. Per ulteriori informazioni, consulta [AWS ConfigRegole supportate da AWS Audit Manager](#) e [AWS Security Hubcontrolli supportati da AWS Audit Manager](#).
 - Attività utente: l'attività utente che modifica la configurazione di una risorsa viene acquisita dai log di CloudTrail nel momento in cui si verifica. 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 CloudTrailnomi degli eventi supportati da AWS Audit Manager](#).
 - 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. Per ulteriori informazioni, consulta [Chiamate API supportate da AWS Audit Manager](#).
- Prova manuale: si tratta delle prove che aggiungi tu stesso ad Audit Manager. Esistono tre modi per aggiungere le proprie prove:
 - Importazione di un file da Amazon S3
 - Caricamento di un file dal proprio browser
 - 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 Audit Manager raccoglie le prove con frequenze diverse a seconda del tipo di prova e dell'origine dati sottostante. Per ulteriori informazioni sulla raccolta dati, consulta

[Come AWS Audit Manager raccoglie le prove](#). Per istruzioni su come esaminare le prove in una valutazione, consulta [Revisione dei controlli in una valutazione](#).

Metodo di raccolta delle prove

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

- I controlli automatici raccolgono automaticamente le prove dalle origini dati AWS. Queste prove automatiche possono aiutare a dimostrare la conformità totale o parziale al controllo.
- I controlli manuali richiedono [il caricamento delle proprie prove](#) 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 Audit Manager 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 Audit Manager con le tue prove.

Ad esempio:

- Il [framework delle best practice dell'IA generativa AWS](#) contiene 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 allarmi CloudWatch siano abilitati per l'Account AWS 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 Audit Manager salva i file esportati da Evidence Finder. Per ulteriori informazioni, consulta [Destinazione di esportazione \(facoltativo\)](#).

F

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Framework

Un framework di Audit Manager è un file utilizzato per strutturare e automatizzare le valutazioni in base a uno specifico standard o principio di governance del rischio. Questi framework aiutano a mappare le risorse AWS in base ai requisiti di un controllo. Includono una raccolta di controlli predefiniti o definiti dal cliente. La raccolta contiene descrizioni e procedure di test per ogni controllo. I controlli sono organizzati e raggruppati in base ai requisiti dello standard o della normativa di conformità specificata. Gli esempi comprendono PCI DSS e GDPR.

Esistono due tipi di framework in Audit Manager:

- Framework standard: framework predefiniti basati sulle best practice AWS per vari standard e normative di conformità. È possibile utilizzare questi framework per facilitare la preparazione degli audit.
- Framework personalizzati: framework personalizzati definiti dall'utente in qualità di Audit Manager. È possibile utilizzare questi framework per facilitare la preparazione degli audit in base ai requisiti specifici di conformità o governance del rischio.

Per istruzioni su come creare e gestire i framework, consulta [Libreria Framework](#).

Note

AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e normative di conformità. Tuttavia, non esegue valutazioni di conformità. Pertanto, le prove raccolte tramite AWS Audit Manager potrebbero non includere tutte le informazioni sull'utilizzo di AWS necessarie per gli audit. AWS Audit Manager non sostituisce i consulenti legali o gli esperti di conformità.

Condivisione del framework

È possibile utilizzare la [funzionalità di condivisione dei framework personalizzati](#) di Audit Manager per condividere rapidamente i framework personalizzati tra Account AWS e regioni. 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, Audit Manager replica il framework personalizzato condiviso nella sua libreria di framework. Oltre a replicare il framework personalizzato, Audit Manager 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. Audit Manager non replica framework o controlli ordinari. Questo perché si tratta di risorse già disponibili per impostazione predefinita in ogni account e regione.

R

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Risorsa

Una risorsa è una risorsa fisica o informativa che viene valutata in un audit. Esempi di risorse AWS 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, Audit Manager 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 controllo di conformità](#) per i controlli che utilizzano AWS Config e 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:

- **Non conforme:** si riferisce a 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 hanno problemi di controllo della conformità. Ciò accade se Security Hub riporta un risultato Pass per la risorsa o se AWS Config riporta un risultato Conforme.
- **Non conclusivo:** si riferisce a risorse per le quali un controllo di conformità non è disponibile o applicabile. Ciò accade se AWS Config 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 API AWS o CloudTrail).

S

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Servizio in ambito

Questo è un Servizio AWS incluso nell'ambito della tua valutazione. Quando specifichi che un servizio è incluso nell'ambito della tua valutazione, Audit Manager valuta le risorse del servizio. Audit Manager è in grado di valutare un'ampia varietà di risorse provenienti da un servizio in ambito. Esempi di risorse sono:

- Un'istanza di Amazon EC2
- Un bucket S3
- Un utente o un ruolo
- 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

Quando utilizzi la console Audit Manager per creare o aggiornare una valutazione da un framework standard, per impostazione predefinita l'elenco dei Servizi AWS in ambito è preselezionato. L'elenco non può essere modificato. Questo perché Audit Manager mappa e seleziona automaticamente le origini dati e i servizi per l'utente. La selezione viene effettuata in base ai requisiti del framework standard. Se un framework standard contiene solo controlli manuali, non ci sono Servizi AWS in ambito per la valutazione e non è possibile aggiungere alcun servizio alla valutazione.

Se è necessario modificare l'elenco dei servizi in ambito per un framework standard, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Note

Occorre tenere presente che un servizio in ambito è diverso da un tipo di origine dati, che può anche essere un Servizio AWS o qualcos'altro. Per ulteriori informazioni, consulta [Qual è la differenza tra un servizio in ambito e un tipo di origine dati?](#) nella sezione Risoluzione dei problemi di questa guida.

Come AWS Audit Manager raccoglie le prove

Ogni valutazione attiva in AWS Audit Manager raccoglie automaticamente prove da una serie di origini dati. Ogni valutazione ha un ambito definito che specifica gli Servizi AWS e gli account da cui Audit Manager raccoglie i dati. Ciascuno di questi servizi e account in ambito contiene più risorse e ogni risorsa è un inventario delle risorse di sistema di tua proprietà. La raccolta delle prove in Audit Manager implica la valutazione di ogni risorsa in ambito. Questa operazione viene definita valutazione della risorsa.

I passaggi seguenti descrivono come Audit Manager raccoglie le prove per ogni valutazione della risorsa:

1. Valutazione di una risorsa dall'origine dati

Per avviare la raccolta delle prove, Audit Manager valuta una risorsa in ambito da un'origine dati. A tale scopo, acquisisce un'istantanea della configurazione, il relativo risultato del controllo di conformità e qualsiasi attività 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 [Prova](#) nella sezione [AWS Audit Manager Concetti e terminologia](#) di questa guida.

2. Conversione dei risultati della valutazione in prova

Il risultato della valutazione della risorsa contiene sia i dati originali acquisiti da quella risorsa, sia i metadati che indicano il controllo supportato dai dati. AWS Audit Manager converte i dati originali in un formato adatto ai revisori. I dati e i metadati convertiti vengono quindi salvati come prove di Audit Manager prima di essere associati a un controllo.

3. Associazione delle prove al relativo controllo

Audit Manager legge i metadati delle prove. Quindi, allega le prove salvate a un controllo correlato all'interno della valutazione. La prova associata diventa visibile in Audit Manager. 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 Audit Manager. Quando la stessa prova è associata a più controlli, Audit Manager 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 Audit Manager può avere più prove provenienti da più origini dati.

Frequenza di raccolta delle prove

La raccolta delle prove è un processo continuo che inizia quando si crea la propria valutazione. AWS Audit Manager raccoglie prove da più origini dati con frequenze diverse. Di conseguenza, non esiste una risposta valida per tutti per quanto riguarda la 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 AWS Security Hub, la frequenza di raccolta delle prove segue la pianificazione dei controlli di 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 Audit Manager, consulta [AWS Security Hub controlli supportati da AWS Audit Manager](#).

- Per AWS Config, la frequenza di raccolta delle prove segue i trigger definiti nelle regole AWS Config. Per ulteriori informazioni sui trigger delle regole AWS Config, consulta [Tipi di trigger](#) nella AWS ConfigGuida per l'utente. Per ulteriori informazioni sui Regole di AWS Config supportati da Audit Manager, consulta [Regole di AWS Config supportato da AWS Audit Manager](#).
- Attività utente: Audit Manager raccoglie questo tipo di prove da 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 Audit Manager. 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 [Libreria di controllo](#). Per ulteriori informazioni su come Audit Manager utilizza le chiamate API per creare prove, consulta [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 controlli AWS Audit Manager

Puoi consultare gli esempi in questa pagina per ulteriori informazioni su come funzionano i controlli in AWS Audit Manager. Questi esempi descrivono l'aspetto di un controllo, il modo in cui Audit Manager genera le prove per quel controllo e i passaggi successivi che si possono compiere per dimostrare la conformità.

Tip

Ti consigliamo di abilitare AWS Config e AWS Security Hub per un'esperienza ottimale in Audit Manager. Se abiliti questi servizi, possono essere utilizzati come tipo di origine dati per i controlli nelle tue valutazioni Audit Manager. In altre parole, Audit Manager può utilizzare i risultati di Security Hub e Regole di AWS Config per 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 Audit Manager possa importare i risultati per tutti gli standard di conformità supportati.

- Dopo aver [abilitato AWS Config](#), assicurati di [abilitare anche il relativo Regole di AWS Config](#) 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 Regole di AWS Config supportati che sono stati abilitati.

Sono disponibili esempi per ciascuno dei seguenti tipi di controlli:

Argomenti

- [Controlli automatici che utilizzano AWS Security Hub come tipo di origine dati](#)
- [Controlli automatici che utilizzano AWS Config come tipo di origine dati](#)
- [Controlli automatici che utilizzano le chiamate API AWS come tipo di origine dati](#)
- [Controlli automatici che utilizzano AWS CloudTrail come tipo di origine dati](#)
- [Controlli manuali](#)
- [Controlli con tipi di origini dati misti \(automatici e manuali\)](#)

Controlli automatici che utilizzano 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 ad allineare il tuo ambiente AWS ai requisiti FSBP.

Esempio di dettagli di controllo

- Nome del controllo: IAM policies should not allow full "*" administrative privileges
- Set di controlli: questo controllo appartiene al set di controlli IAM. Si tratta di un raggruppamento di controlli relativi alla gestione delle identità e degli accessi.
- Tipo di origine dati: AWS Security Hub
- Tipo di prova: controllo di conformità

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

Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
<ul style="list-style-type: none"> IAM (8) <ul style="list-style-type: none"> IAM policies should not allow full "*" administrative privileges 	Active	-	0	0
	Under review	-	0	0

La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo e quante di tali prove sono incluse nel report di valutazione. 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 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 Audit Manager raccoglie le prove per questo controllo

Audit Manager adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager valuta le risorse in ambito. A tale scopo, utilizza l'origine dati specificata nelle impostazioni di controllo. In questo esempio, le tue policy IAM sono la risorsa e Security Hub e AWS Config sono il tipo di origine dati. Audit Manager cerca il risultato di uno specifico controllo di Security Hub ([IAM.1](#)), che a sua volta utilizza una regola AWS Config per valutare le tue 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. Audit Manager 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. Audit Manager allega le prove salvate al controllo nella tua valutazione denominata IAM policies should not allow full "*" administrative privileges.

Come utilizzare Audit Manager 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 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 ad allineare il tuo ambiente AWS ai 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 utilizzano 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 possono contribuire ad allineare AWS all'ambiente ai Guardrail AWS Control Tower.

Esempio di dettagli di controllo

- Nome del controllo: 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.
- Tipo di origine dati: AWS Config
- Tipo di prova: controllo di conformità

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

Control sets (1/5)		Delegate control set		Complete control set review	
Q Disallow public write access to S3 buckets X 1 match					
Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report	
○ Disallow public access (4)	☺ Active	-	0	0	
4.1.2 - Disallow public write access to S3 buckets	⌚ Under review	-	0	0	

La valutazione mostra lo stato del controllo, il numero di prove raccolte finora per questo controllo e quante di tali prove sono incluse nel report di valutazione. 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 del bucket S3 sono troppo permissivi 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 Audit Manager raccoglie le prove per questo controllo

Audit Manager adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager 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 il tipo di origine dati. Audit Manager cerca il risultato di una regola AWS Config specifica ([s3-bucket-public-write-prohibited](#)) per valutare le impostazioni, la policy 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 una prova di controllo di conformità per i controlli che utilizzano AWS Config come tipo di origine dati. La prova contiene il risultato del controllo di conformità riportato direttamente da AWS Config.
3. Audit Manager allega le prove salvate al controllo nella tua valutazione denominata 4.1.2 - `Disallow public write access to S3 buckets`.

Come utilizzare Audit Manager 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 di AWS Config che afferma che un bucket S3 è non 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 ad allineare l'ambiente AWS ai requisiti 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. È quindi possibile condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

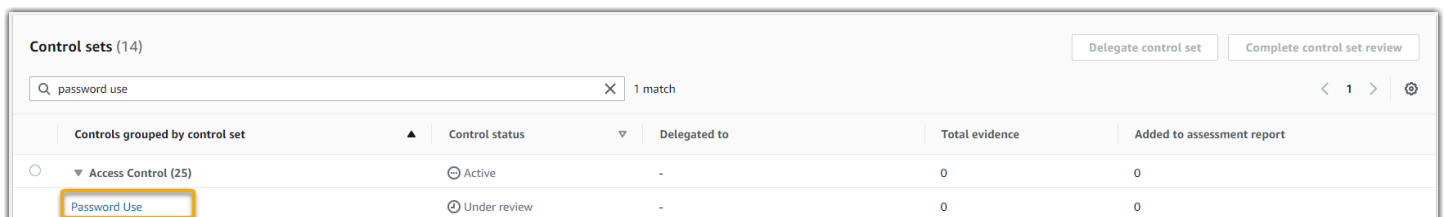
Controlli automatici che utilizzano le chiamate API AWS come tipo di origine dati

Questo esempio mostra un controllo personalizzato che utilizza le chiamate API AWS come tipo di origine dati. Audit Manager utilizza questo controllo per generare prove che possono contribuire ad allineare l'ambiente AWS ai 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.
- Tipo di origine dati: AWS Chiamate API
- Tipo di prova: dati di configurazione

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



Control sets (14)					
<input type="text" value="password use"/>		1 match			
Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report	
▼ Access Control (25)	⊖ Active	-	0	0	
Password Use	⊖ Under review	-	0	0	

La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo e quante di tali prove sono incluse nel report di valutazione. 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 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. Audit Manager 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 Audit Manager raccoglie le prove per questo controllo

Audit Manager adotta le seguenti misure per raccogliere prove per questo controllo personalizzato:

1. Per ogni controllo, Audit Manager valuta le risorse in ambito utilizzando l'origine dati specificata nelle impostazioni di controllo. In questo caso, i principi IAM sono le risorse e le chiamate API AWS 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. Audit Manager 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. Audit Manager allega le prove salvate al controllo personalizzato nella tua valutazione denominata Password Use.

Come utilizzare Audit Manager 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 risposta [GetAccountPasswordPolicy](#) 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 policy di controllo dell'accesso tramite password sufficienti per gli 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. È quindi possibile condividere il report con i revisori per dimostrare che il controllo funziona come previsto.

Controlli automatici che utilizzano 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 preso dal [framework HIPAA](#). Audit Manager 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)
- Set di controlli: questo controllo appartiene al set di controlli chiamato 164.308 Administrative Safeguards.
- Tipo di origine dati: AWS CloudTrail
- Tipo di prova: attività dell'utente

Ecco il controllo mostrato all'interno di una valutazione di Audit Manager creata dal framework HIPAA:

Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
164.308 Administrative Safeguards (22)	Active	-	0	0
164.308(a)(5)(ii)(C)	Under review	-	0	0

La valutazione mostra lo stato del controllo. Mostra anche quante prove sono state raccolte finora per questo controllo e quante di tali prove sono incluse nel report di valutazione. 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 una procedura di monitoraggio per rilevare accessi inappropriati. Un esempio di accesso inappropriato si ha quando qualcuno inserisce più combinazioni di nomi utente o password per tentare di accedere a un sistema informativo. Audit Manager aiuta a convalidare questo controllo fornendo un elenco di tutti i tentativi di accesso rilevati per le risorse che rientrano nell'ambito della valutazione.

In che modo Audit Manager raccoglie le prove per questo controllo

Audit Manager adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager valuta le risorse in ambito utilizzando l'origine dati specificata nelle impostazioni di controllo. In questo caso, gli utenti sono la risorsa e CloudTrail è il tipo di origine dati. Audit Manager cerca il risultato di tutti gli [eventi di accesso alla Console di gestione AWS](#) registrati 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 le prove dell'attività degli utenti per i controlli che utilizzano CloudTrail come tipo di origine dati. La prova contiene i dati originali acquisiti dagli utenti e metadati aggiuntivi che indicano il controllo supportato dai dati.
3. Audit Manager allega le prove salvate al controllo nella tua valutazione denominata 164.308(a)(5)(ii)(C).

Come utilizzare Audit Manager 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, è possibile esaminare le prove per vedere gli eventi di accesso registrati da CloudTrail. Il log descrive l'attività di accesso alla console degli utenti, e include le seguenti informazioni:

- Ogni accesso riuscito
- Ogni tentativo di accesso non riuscito
- Verifica di quando è stata applicata l'autenticazione a più fattori (MFA)
- L'indirizzo IP di ogni evento di accesso

Puoi utilizzare questo log come prova per dimostrare che disponi di procedure di monitoraggio sufficienti per gli Account AWS che rientrano nell'ambito della valutazione. Se lo desideri, puoi anche fornire ulteriori commenti su queste policy aggiungendo un commento al controllo. Ad esempio, se il log mostra discrepanze come più tentativi di accesso non riusciti, puoi aggiungere un commento che descriva come è stato 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 ad allineare l'ambiente AWS ai 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. È quindi possibile 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 Audit Manager non raccoglie prove automatiche. Si tratta di un controllo standard preso dal [framework NIST 800-53 \(Rev. 5\)](#). È possibile utilizzare Audit Manager per caricare e memorizzare le prove che dimostrano la conformità per questo controllo.

Esempio di dettagli di controllo

- Nome del controllo: PS-4(1) - Post-employment Requirements
- Set di controlli: questo controllo appartiene al set di controlli Personnel Termination. Si tratta di un raggruppamento di controlli relativi alla sicurezza delle informazioni nel contesto delle procedure di licenziamento.
- Tipo di origine dati: manuale
- Tipo di prova: manuale

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

Control sets (1/280)		Delegate control set		Complete control set review	
Q PS-4(1) X 1 match					
Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report	
Personnel Termination (3)	Active	-	0	0	
PS-4(1) - Post-employment Requirements	Under review	-	0	0	

La valutazione mostra lo stato del controllo. Mostra anche quante prove siano state raccolte finora per questo controllo e quante di tali prove siano incluse nel report di valutazione. 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 confermare che si sta proteggendo le informazioni organizzative in caso di licenziamento di un dipendente. In particolare, è possibile dimostrare di aver

costantemente informato le persone licenziate dei requisiti post-impiego applicabili e legalmente vincolanti per la protezione delle informazioni dell'organizzazione. Inoltre, è possibile dimostrare che tutte le persone licenziate firmano una dichiarazione di accettazione dei requisiti post-impiego come parte del processo di licenziamento dell'organizzazione.

Come caricare manualmente le prove per questo controllo

È possibile eseguire le seguenti operazioni per caricare prove manuali a supporto di questo controllo:

1. Inserire le prove manuali che si desidera caricare in un bucket Amazon Simple Storage Service (S3) e annotare l'URI S3.
2. Nella valutazione di Audit Manager, aprire il controllo, andare alla scheda delle cartelle delle prove e caricare le prove inserendo l'URI S3. Per istruzioni, consulta [Caricamento delle prove manuali in AWS Audit Manager](#).
3. Audit Manager crea una cartella delle prove che prende il nome dalla data di caricamento delle prove. Quindi allega le prove salvate al controllo nella valutazione denominata PS-4(1) - Post-employment Requirements.

Come utilizzare Audit Manager per dimostrare la conformità a questo controllo

Se si dispone di documentazione che supporta questo controllo, è possibile caricarla come prova manuale. Ad esempio, è possibile caricare la copia più recente dei requisiti legalmente vincolanti post-impiego che il dipartimento delle Risorse Umane rilascia ai dipendenti licenziati. Se qualcuno è stato licenziato durante il periodo di audit, è anche possibile caricare copie datate indirizzate a tali persone.

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 hai una lettera di conferma firmata dalla persona licenziata. Potresti delegare il controllo a una parte interessata delle Risorse Umane, che potrà quindi caricare una copia della lettera firmata. Oppure, se nessun dipendente è stato licenziato durante il periodo di audit, puoi lasciare un commento che spieghi perché al controllo non sono allegate lettere firmate.

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)

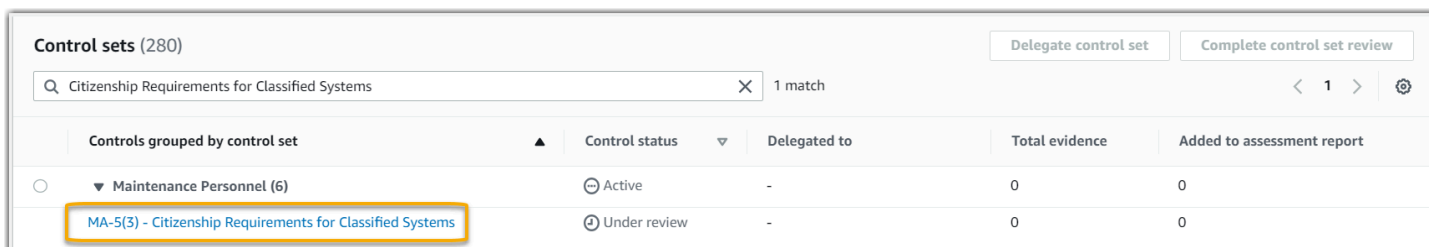
In molti casi, è necessaria una combinazione di prove automatiche e manuali per soddisfare un controllo. Sebbene Audit Manager sia in grado di fornire prove automatiche pertinenti al controllo, potrebbe essere necessario integrare questi dati con prove manuali che l'utente identifica e carica personalmente.

Questo esempio mostra un controllo che utilizza una combinazione di prove manuali e prove automatiche provenienti da chiamate API AWS. Si tratta di un controllo standard preso dal [framework NIST 800-53 \(Rev. 5\)](#). Audit Manager 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: MA-5(3) - Citizenship Requirements for Classified Systems
- Set di controlli: questo controllo appartiene al set di controlli Maintenance Personnel. Si tratta di un raggruppamento di controlli che si riferisce alle persone che eseguono la manutenzione hardware o software dei sistemi organizzativi.
- Tipo di origine dati: AWSchiamate API e prove manuali supplementari
- Tipo di prova: dati di configurazione

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



Control sets (280)		Delegate control set	Complete control set review
<input type="text" value="Citizenship Requirements for Classified Systems"/> 1 match			
Controls grouped by control set	Control status	Delegated to	Total evidence
<input type="radio"/> Maintenance Personnel (6)	Active	-	0
<input type="radio"/> MA-5(3) - Citizenship Requirements for Classified Systems	Under review	-	0

La valutazione mostra lo stato del controllo. Mostra anche quante prove siano state raccolte finora per questo controllo e quante di tali prove siano incluse nel report di valutazione. 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 aiutare a garantire che il personale che esegue le attività di manutenzione e diagnostica abbia lo status di cittadinanza richiesto. Se il sistema elabora,

memorizza o trasmette informazioni classificate, è necessario dimostrare che il personale addetto alla manutenzione ha la cittadinanza statunitense. Audit Manager aiuta a convalidare la dimostrazione. A tale scopo, restituisce un elenco completo di tutte le policy e i principi IAM che rientrano nell'ambito della valutazione. Sarà quindi possibile verificare e dimostrare che gli utenti di questo elenco posseggono i requisiti di cittadinanza necessari. Per farlo è possibile caricare manualmente prove supplementari del loro status di cittadinanza.

In che modo Audit Manager raccoglie le prove per questo controllo

Audit Manager adotta le seguenti misure per raccogliere prove per questo controllo:

1. Per ogni controllo, Audit Manager valuta le risorse in ambito utilizzando l'origine dati specificata nelle impostazioni di controllo. In questo caso, le policy e i principi IAM sono le risorse e le chiamate API AWS sono l'origine dati. [Audit Manager cerca il risultato di quattro chiamate API IAM specifiche \(ListUsers/ListRoles/ListGroups/ListPolicies\) e restituisce un elenco delle policy e dei principi IAM 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 dei dati di configurazione per i controlli che utilizzano le chiamate API come tipo di origine dati. La prova contiene i dati originali acquisiti dalle risposte API e metadati aggiuntivi che indicano il controllo supportato dai dati.
3. Audit Manager allega le prove salvate al controllo nella tua valutazione denominata MA-5(3) - Citizenship Requirements for Classified Systems.

Come caricare manualmente le prove per questo controllo

È possibile eseguire le seguenti operazioni per caricare prove manuali a integrazione delle prove automatiche:

1. Inserire la documentazione di cittadinanza in un bucket Amazon Simple Storage Service (Amazon S3) e annotare l'URI S3.
2. Nella valutazione di Audit Manager, aprire il controllo, andare alla scheda delle cartelle delle prove e caricare le prove. Per farlo, inserire l'URI S3. Per istruzioni, consulta [Aggiunta di prove manuali in AWS Audit Manager](#).
3. Audit Manager allega le prove caricate al controllo nella valutazione denominata MA-5(3) - Citizenship Requirements for Classified Systems.

Come utilizzare Audit Manager 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, dall'esame delle prove si deduce un elenco di 20 utenti. Se non si è sicuri di come identificare gli utenti che sono addetti alla manutenzione o la loro cittadinanza, è possibile delegare il controllo a un esperto in materia per la convalida. Il delegato può confermare l'elenco del personale addetto alla manutenzione e caricare manualmente prove supplementari come documentazione del loro status di cittadinanza. La conferma della cittadinanza di tutti gli utenti pertinenti dell'elenco aiuta ad allineare l'ambiente AWS ai requisiti NIST. In alternativa, se il sistema non elabora, memorizza o trasmette informazioni classificate, è possibile lasciare un commento che spieghi perché questo controllo non è applicabile.

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 Servizi AWS correlati

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

AWS Security Hub

AWS Security Hub monitora l'ambiente utilizzando controlli di sicurezza automatici basati sulle best practice AWS e sugli standard del settore. Audit Manager 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, consulta [Che cos'è AWS Security Hub?](#) nella Guida per l'utente AWS Security Hub.

AWS CloudTrail

AWS CloudTrail aiuta a monitorare le chiamate effettuate alle risorse AWS del proprio account. Queste includono le chiamate effettuate dalla Console di gestione AWS, dalla CLI AWS e altri Servizi AWS. Audit Manager raccoglie i dati del log direttamente da CloudTrail e converte i log elaborati in prove delle attività degli utenti. Per ulteriori informazioni su CloudTrail, consulta [Cos'è AWS CloudTrail?](#) nella Guida per l'utente AWS CloudTrail.

AWS Config

AWS Config fornisce una panoramica dettagliata della configurazione delle risorse AWS nel 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 della posizione di sicurezza delle risorse riportando i risultati direttamente da AWS Config. Per ulteriori informazioni su AWS Config, consulta [Che cos'è AWS Config?](#) nella Guida per l'utente AWS Config.

AWS License Manager

AWS License Manager ottimizza il processo per trasferire le licenze di fornitore software nel cloud. Quando si costruisce un'infrastruttura cloud su AWS, è possibile risparmiare sui costi riutilizzando l'inventario delle licenze esistenti per utilizzarle con le risorse cloud. Audit Manager 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 [Che cos'è AWS License Manager?](#) nella AWS License Manager Guida per l'utente.

AWS Control Tower

AWS Control Tower impone guardrail preventivi e investigativi per l'infrastruttura cloud. Audit Manager fornisce un AWS Control Tower framework Guardrail per assistere nella preparazione dell'audit. Il framework contiene tutte le regole AWS Config basate sui guardrail di AWS Control Tower. Per ulteriori informazioni su AWS Control Tower, consulta [Che cos'è AWS Control Tower?](#) nella AWS Control Tower Guida 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 AWS soddisfa i requisiti di conformità. Per contro, 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 [Che cos'è AWS Artifact?](#) nella AWS Artifact Guida per l'utente. È possibile scaricare un [elenco di AWS report](#) in AWS Management Console.

Per un elenco di Servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consulta [Servizi AWS coperti dal 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 utilizzo AWS direttamente nel tuo ambiente GRC. Ciò semplifica il modo in cui gestisci 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 Audit Manager. È inoltre possibile vedere un riferimento delle azioni API di Audit Manager che si possono eseguire direttamente all'interno di tali prodotti.

Argomenti

- [Comprensione del funzionamento delle integrazioni di terze parti con Audit Manager](#)
- [Prodotti partner GRC di terze parti che si integrano con Audit Manager](#)

Comprensione del funzionamento delle integrazioni di terze parti con Audit Manager

I partner GRC possono utilizzare le API pubbliche di Audit Manager per integrare i loro prodotti con Audit Manager. Con questa integrazione, puoi mappare i controlli aziendali del tuo ambiente GRC ai controlli forniti da Audit Manager.

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

Quando si utilizza un'integrazione Audit Manager 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 Audit Manager](#).
- Tutte le risorse Audit Manager create nel prodotto partner GRC si riflettono anche in Audit Manager.

- Sei soggetto a [AWS Audit Manager prezzi aggiuntivi](#) oltre a quelli del prodotto GRC di terze parti.
- Le prove raccolte da Audit Manager sono immutabili. Le prove vengono presentate esattamente nello stesso modo nei prodotti GRC di terze parti come nella console di Audit Manager. 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 Audit Manager](#) si applicano anche all'interno del prodotto GRC di terze parti. Ad esempio, ogni Account AWS può avere fino a 100 valutazioni Audit Manager attive. Questa quota a livello di account si applica indipendentemente dal fatto che le valutazioni siano state create nella console di Audit Manager o nel prodotto GRC di terze parti. La maggior parte delle quote Audit Manager, ma non tutte, è elencata nello spazio dei nomi AWS Audit Manager nella console Service Quotas. Per sapere come richiedere un aumento delle quote, consulta [Gestione delle proprie quote di Audit Manager](#).

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

Prodotti partner GRC di terze parti che si integrano con Audit Manager

I seguenti prodotti GRC di terze parti possono acquisire prove da Audit Manager.

MetricStream

Per utilizzare questa integrazione, contatta [MetricStream](#) per l'accesso e l'acquisto del software GRC MetricStream.

Basata sulla piattaforma MetricStream, la soluzione GRC MetricStream Enterprise consente un approccio completo e collaborativo alle attività e ai processi GRC a livello aziendale. Inserendo le prove di Audit Manager in MetricStream, è possibile identificare in modo proattivo le prove non conformi dal proprio ambiente AWS ed esaminarle insieme alle prove provenienti dalle proprie origini 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 l'integrazione di MetricStream e Audit Manager, puoi eseguire le seguenti operazioni API.

Attività	Operazione API
Configurazione dell'integrazione di Audit Manager	<ul style="list-style-type: none"> • GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Esame delle risorse di Audit Manager	<ul style="list-style-type: none"> • GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Creazione di risorse Audit Manager	<ul style="list-style-type: none"> • CreateAssessment • CreateAssessmentFramework
Aggiornamento di risorse Audit Manager	<ul style="list-style-type: none"> • UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Gestione delle prove	<ul style="list-style-type: none"> • StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)
Eliminazione di risorse Audit Manager	<ul style="list-style-type: none"> • DeleteAssessmentFramework

Links MetricStream correlati


- [Marketplace AWS link](#)
- [Link al prodotto](#)
- [Prezzo del prodotto](#)

Utilizzo di Audit Manager con un SDK AWS

I Software Development Kit (SDK) di AWS sono disponibili per molti dei linguaggi di programmazione più diffusi. 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	Documentazione specifica per Audit Manager	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 (Boto3) 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 per Audit Manager, consulta [Esempi di codice per AWS Audit Manager](#).

 **Note**

Audit Manager 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.

Configurazione AWS Audit Manager

Prima di iniziare a utilizzare Audit Manager, assicurati di aver completato le seguenti attività di configurazione.

Argomenti

- [Prerequisiti: creare Account AWS e impostare le autorizzazioni](#)
- [Abilita Audit Manager: utilizza la console AWS CLI, l'API o l'API per abilitare Audit Manager](#)
- [Consigli: configura le integrazioni consigliate con altri Servizi AWS](#)

Prerequisiti

Segui questi passaggi per creare un utente Account AWS e un utente amministrativo con privilegi di configurazione di Audit Manager.

Fasi

- [Iscriviti per un Account AWS](#)
- [Crea un utente con accesso amministrativo](#)
- [Aggiungi le autorizzazioni necessarie per accedere e abilitare Audit Manager](#)

Important

Se hai già configurato AWS un IAM, puoi saltare i passaggi 1 e 2. Tuttavia, è necessario completare la fare 3 per assicurarti di disporre delle autorizzazioni necessarie per configurare Audit Manager.

Iscriviti 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 AWS viene 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, assegna l'accesso amministrativo a un utente e utilizza 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 Console](#) come 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 Audit Manager

È necessario fornire agli utenti le autorizzazioni necessarie per abilitare Audit Manager.

Per gli utenti che necessitano dell'accesso completo a Audit Manager, utilizza la policy [AWSAuditManagerAdministratorAccess](#) gestita. 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 AWS](#) nella Guida 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.

Abilita AWS Audit Manager

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 Audit Manager tramite la console

1. Apri la console 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.

Security, Identity, & Compliance, Management & Governance

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

Launch AWS Audit Manager

Start from a pre-built standard framework based on common compliance standards and developed with AWS best practices in mind.

[Set up AWS Audit Manager](#)

4. In Autorizzazioni, non è richiesta alcuna azione. Ciò perché Audit Manager 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.

Permissions

AWS Audit Manager uses a service-linked role to connect to data sources on your behalf, and no action is required by default. To learn more about the type of permissions available in AWS Audit Manager, view [How AWS Audit Manager works with IAM](#).

[View IAM service-linked role permission](#)

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.

Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)

Se desideri utilizzare la tua chiave gestita dal cliente per crittografare i dati in Audit Manager, seleziona la casella di controllo accanto a Personalizza le impostazioni di crittografia (avanzate). Puoi selezionare una chiave KMS esistente o [crearne una nuova](#).

Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

Customize encryption settings (advanced)
To use the default key, clear this option.

Choose an AWS KMS key
This key will be used for encryption instead of the default key.

6. (Facoltativo) In Amministratore delegato: facoltativo, è possibile specificare un account amministratore delegato se si desidera che Audit Manager esegua valutazioni per più account. Per ulteriori informazioni e consigli, consulta [Abilitare e configurare AWS Organizations per l'uso con Audit Manager](#).

Delegated administrator - optional

For AWS Audit Manager to support multiple accounts in your organization, you must specify a delegated administrator. Use this setting to add or remove the delegated AWS Audit Manager administrator for your organization. [Learn more](#)

Delegated administrator account ID

7. (Facoltativo) Nella sezione AWS Config «opzionale», ti consigliamo di AWS Config abilitarla per un'esperienza ottimale. Ciò consente all'Audit Manager di generare prove utilizzando AWS Config le regole. Per istruzioni e impostazioni consigliate, consulta [Attivare e configurare AWS Config per l'uso con Audit Manager](#).

AWS Config - optional

Allow AWS Audit Manager to access [AWS Config](#) and generate evidence from AWS Config rules. Enabling AWS Config incurs charges.

8. (Facoltativo) In Security Hub: facoltativo, ti consigliamo di abilitare Security Hub per un'esperienza ottimale. Ciò consente all'Audit Manager di generare prove utilizzando i controlli Security Hub. Per istruzioni e impostazioni consigliate, consulta [Attivare e configurare AWS Security Hub per l'uso con Audit Manager](#).

Security Hub - optional

Allow AWS Audit Manager to access [Security Hub](#) and generate evidence from security findings. Enabling Security Hub incurs charges.

Enable Security Hub 

- Scegli Configurazione completa per completare il processo di configurazione.

Complete setup

AWS CLI

Per abilitare Audit Manager utilizzando il 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 dell'Audit Manager utilizzando la tua chiave gestita dal cliente. Se non specifichi un'opzione qui, Audit Manager 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 Audit Manager. 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 Audit Manager tramite l'API Audit Manager

Utilizzare l'[RegisterAccount](#) operazione con i seguenti parametri di configurazione:

- [kmsKey](#) (facoltativo): utilizza questo parametro per crittografare i dati dell'Audit Manager utilizzando la tua chiave gestita dal cliente. Se non specifichi un'opzione qui, Audit Manager 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"
}
```

Raccomandazioni

Per un'esperienza ottimale in Audit Manager, consigliamo di configurare e abilitare le seguenti funzionalità Servizi AWS.

Argomenti

- [Imposta le funzionalità consigliate di Audit Manager](#)
- [Configura le integrazioni consigliate con altri Servizi AWS](#)

Imposta le funzionalità consigliate di Audit Manager

Dopo aver abilitato Audit Manager, ti consigliamo di attivare la funzionalità di ricerca delle prove.

[Evidence finder](#) fornisce un modo efficace per cercare prove in Audit Manager. 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.

Per utilizzare evidence finder, è necessario abilitare questa funzionalità dalle impostazioni di Audit Manager. Per istruzioni, consulta [Impostazioni di evidence finder](#).

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 Audit Manager su più account e consolidare le prove in un account amministratore delegato.
- **AWS Security Hubs e AWS Config—** Quando li abiliti Servizi AWS, possono essere utilizzati come tipo di origine dati per i controlli nelle valutazioni dell'Audit Manager. Audit Manager può quindi riportare i risultati dei controlli di conformità direttamente da questi servizi.

Argomenti

- [Abilita e configura AWS Config \(facoltativo\)](#)
- [Abilita e configura AWS Security Hub \(facoltativo\)](#)
- [Abilita AWS Organizations \(opzionale\)](#)

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.

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

Important

L'abilitazione AWS Config è una raccomandazione facoltativa. Tuttavia, se abiliti AWS Config, sono necessarie le seguenti impostazioni.

Dopo l'attivazione AWS Config, assicurati di [abilitare anche AWS Config le regole](#) o di [implementare un pacchetto di conformità](#) per lo standard di conformità correlato al tuo audit. Questa fase garantisce che Audit Manager 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 Config](#) per 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-rotated](#) regola 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 Audit Manager 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 Audit Manager. Se Audit Manager 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.

Audit Manager non gestisce Security Hub per te. Puoi seguire queste fasi per abilitare Security Hub e configurarne le 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 Audit Manager](#)

Fase 1: Abilita AWS Security Hub

Puoi abilitare Security Hub utilizzando sia la console che l'API. Per istruzioni, consulta [Configurazione di AWS Security Hub](#) nella Guida per l'utente AWS Security Hub .

Fase 2: configurazione delle impostazioni Security Hub da utilizzare con Audit Manager

Important

L'attivazione di Security Hub è un consiglio facoltativo. Tuttavia, se abiliti Security Hub, sono necessarie le seguenti impostazioni.

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](#): questa fase 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 Audit Manager. Di conseguenza, i risultati consolidati comportano una diminuzione delle valutazioni totali delle risorse uniche eseguite da Audit Manager per i risultati Security Hub. Per tale motivo, l'utilizzo di risultati consolidati può spesso portare a una riduzione dei costi di utilizzo dell'Audit Manager. 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 Audit Manager, consulta [Prezzi di AWS Audit Manager](#).

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/](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 Audit Manager.

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 AWS Organizations (opzionale)

Audit Manager supporta più account tramite l'integrazione con AWS Organizations. Audit Manager 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 Audit Manager con l'organizzazione come zona di attendibilità. Solo l'account di gestione può designare un amministratore delegato.

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 Audit Manager](#)

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 caratteristiche nell'organizzazione. Per le istruzioni, consulta la sezione [Abilitazione di tutte le caratteristiche nell'organizzazione](#) nella Guida per l'utente di AWS Organizations .

Fase 3: specificare un amministratore delegato per Audit Manager

Si consiglia di abilitare Audit Manager 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.

Warning

Dopo aver specificato un amministratore delegato utilizzando un account di gestione Organizations, l'account di gestione non può più creare valutazioni aggiuntive in Audit Manager. Inoltre, la raccolta delle prove si interrompe per tutte le valutazioni esistenti create dall'account di gestione. Invece, Audit Manager raccoglie e allega prove all'amministratore delegato, che è l'account principale per la gestione delle valutazioni dell'organizzazione.

Per aggiungere o modificare un amministratore delegato dopo aver abilitato Audit Manager, consulta [AWS Audit Manager impostazioni, Amministratore delegato](#).

Aspetti da valutare:

- Non puoi utilizzare il tuo account di 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 Audit Manager, è necessario designare lo stesso account amministratore delegato in tutte le regioni.
- Se hai fornito una chiave gestita dal cliente quando hai abilitato Audit Manager, assicurati che l'account amministratore delegato abbia accesso a quella chiave KMS. Per rivedere e modificare le impostazioni di crittografia dell'Audit Manager, consulta [Crittografia dei dati](#).
- Per le soluzioni ai problemi più comuni relativi alle Organizzazioni e agli amministratori delegati in Audit Manager, consulta [Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations](#).

Cosa devo fare dopo?

Ora che hai configurato Audit Manager, sei pronto per iniziare a utilizzare il servizio. Puoi anche visitare la pagina delle impostazioni della console per aggiornare le impostazioni che hai scelto durante la configurazione di Audit Manager.

Inizia a usare Audit Manager

Puoi iniziare a usare Audit Manager seguendo un tutorial che ti spiega come creare la tua prima valutazione. Per ulteriori informazioni, consulta [Tutorial for Audit Owners: Creazione di una valutazione](#).

Aggiorna le impostazioni dell'Audit Manager

Puoi aggiornare le tue impostazioni in qualsiasi momento. Per ulteriori informazioni, consulta [Impostazioni di AWS Audit Manager](#).

Guida introduttiva 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 Audit Manager 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 dell'Audit Manager, 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 Audit Manager. Questo perché i proprietari degli audit delegano specifici set di controlli per la revisione e non intere valutazioni.

Per ulteriori informazioni su questi utenti e altri concetti di Audit Manager, consulta [Proprietari dell'audit e Delegati](#) nella sezione [concetti e terminologia AWS Audit Manager](#) di questa guida. Per ulteriori informazioni sulle autorizzazioni IAM consigliate per ogni utente, consulta [Politiche consigliate per gli utenti in AWS Audit Manager](#).

Tutorial Audit Manager

[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 controlli e le relative prove, aggiungere commenti, caricare prove aggiuntive 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, crea una valutazione utilizzando [AWS Audit Manager Framework di esempio](#). Creando una valutazione, si avvia il processo continuo di raccolta automatica delle prove per i controlli di quel framework.

In questo tutorial vengono illustrate le seguenti operazioni:

- [Seleziona un framework standard da cui creare una valutazione](#)
- [Specificate gli AWS account da includere nella valutazione](#)
- [Specificate i AWS servizi da includere nella valutazione](#)
- [Specifica i proprietari dell'audit per la valutazione](#)
- [Rivedi e crea la tua valutazione](#)

Prima di iniziare questo tutorial, assicurati che siano soddisfatte le seguenti condizioni:

- Hai completato tutti i prerequisiti descritti in [Configurazione AWS Audit Manager](#). Devi usare il tuo AWS account e la 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 l'[Esempio 2: consenti l'accesso completo all'amministratore](#) e l'[Esempio 3: consenti l'accesso alla gestione](#).
- Conosci la terminologia e le funzionalità di Audit Manager. Per una panoramica generale, consulta [Cos'è AWS Audit Manager?](#) e [concetti e terminologia AWS Audit Manager](#).

Note

AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici quadri e regolamenti di conformità. Non viene tuttavia 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.

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 Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Scegli Avvia AWS Audit Manager.
3. Nel pannello di navigazione, scegli Nozioni di base, quindi scegli Inizia con un framework.
4. Scegli il framework che desideri, quindi scegli Crea valutazione dal framework. Questo esempio utilizza AWS Audit Manager Framework di esempio.
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. Nella sezione Destinazione dei report di valutazione, scegli il bucket Amazon S3 in cui desideri salvare i report di valutazione.
8. Nella sezione Framework, conferma che AWS Audit Manager Framework di esempio (o il framework di tua scelta) sia selezionato.
9. Nella sezione 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. Per ulteriori informazioni sui tag in AWS Audit Manager, consulta. [Tagging delle risorse AWS Audit Manager](#)
10. Seleziona Successivo.

Passaggio 2: Specificare AWS gli account nell'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 Audit Manager (se non l'hai già fatto), consulta [Abilita 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 AWS Account, seleziona gli AWS account che desideri includere nell'ambito della valutazione.
 - Se hai abilitato Organizations in AWS Audit Manager, vengono elencati più account.
 - Se non hai abilitato Organizations in Audit Manager, viene elencato solo il tuo account attuale.
2. Seleziona Successivo.

Fase 3: Specificare AWS i servizi nell'ambito

Il framework selezionato in precedenza definisce AWS i servizi per i quali Audit Manager monitora e raccoglie prove.

Quando utilizzi la console Audit Manager per creare una valutazione da un framework standard, l'elenco dei servizi inclusi nell'ambito è preselezionato e non può essere modificato. Questo perché Audit Manager mappa e seleziona automaticamente le fonti di dati e i servizi per te. La selezione viene effettuata in base ai requisiti del framework standard. Se un AWS servizio elencato non è selezionato, Audit Manager non raccoglie prove dalle risorse relative a quel servizio. Questo vale anche se è selezionato ma non lo hai iscritto nel tuo ambiente.

In questa fase del tutorial, puoi esaminare quali AWS servizi rientrano nell'ambito della valutazione in base alla definizione del framework. Per ulteriori informazioni sui framework e su come accedervi e rivederli, consulta la sezione [Libreria Framework](#) di questa guida.

Per specificare AWS i servizi inclusi nell'ambito

1. Nella sezione AWS Servizi, consulta l'elenco dei servizi che rientrano nell'ambito di questa valutazione.
2. Seleziona Successivo.

Tip

Se è necessario modificare l'elenco dei servizi inclusi nell'ambito, è possibile farlo utilizzando l'[CreateAssessmentAPI](#) fornita da Audit Manager.

In alternativa, puoi [personalizzare un framework standard](#) e quindi creare una valutazione dal framework personalizzato.

Fase 4: specificare i proprietari dell'audit

In questa fase, l'utente 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 proprietari dell'audit, utilizza la barra di ricerca per nome o account AWS .
2. Seleziona Successivo.

Passaggio 5: 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 avviare la tua prima valutazione e iniziare la raccolta di prove in corso.

Dopo aver creato una valutazione, la raccolta delle prove continua finché non [modifichi lo stato della valutazione](#) e lo imposti 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. AWS Audit Manager raccoglie automaticamente prove da più fonti di dati e la frequenza di tale raccolta di prove si basa sul tipo di prova. Per ulteriori informazioni sul tagging, consulta [Frequenza di raccolta delle prove](#) in questa guida.

A questo punto come si può procedere?

Ti consigliamo di continuare con ulteriori informazioni su concetti e strumenti introdotti in questo tutorial. Puoi farlo consultando le risorse seguenti:

- [Revisione di una valutazione](#) – Presenta la pagina di valutazione in cui puoi esplorare i diversi componenti della valutazione.
- [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 documento, ti consigliamo in particolare di dare un'occhiata ai 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](#)
- [Libreria Framework](#) – Presenta la libreria di framework e spiega come [creare un framework personalizzato](#) per esigenze di conformità specifiche.
- [Libreria di controllo](#) – Presenta la libreria di controlli e spiega come [creare un controllo personalizzato](#) da utilizzare nel framework personalizzato.
- [concetti e terminologia AWS Audit Manager](#) – Fornisce le definizioni dei concetti e della terminologia utilizzati in Audit Manager.
- [Video] [Raccogli prove e gestisci i dati di audit utilizzando 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 proprietari dell'audit utilizzano Audit Manager per creare valutazioni e raccogliere prove per i controlli elencati 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.

In questo tutorial vengono illustrate le seguenti operazioni:

- [Accedere alle notifiche inviate dal proprietario dell'audit](#)
- [Esaminare un set di controlli e le A delegate completes their review and submits the reviewed control set back to the audit ownerrelative prove](#)
- [Caricare prove manuali a supporto di un controllo](#)
- [Aggiungere un commento per un controllo che stai esaminando](#)
- [Aggiornare lo stato di un controllo](#)
- [Inviare il set di controlli revisionato al proprietario dell'audit una volta completata la revisione](#)

Prima di iniziare questo tutorial, assicurati che siano soddisfatte le seguenti condizioni:

- Il tuo AWS account è configurato. Per completare questo tutorial, devi utilizzare sia il tuo AWS account che la AWS Audit Manager console. Per ulteriori informazioni, consulta [Configurazione AWS Audit Manager](#).
- Conosci la terminologia e le funzionalità di Audit Manager. Per una panoramica generale di Audit Manager, consulta [Cos'è AWS Audit Manager?](#) e [concetti e terminologia AWS Audit Manager](#).

Fase 1: accesso alle notifiche

Inizia accedendo a AWS Audit Manager, dove puoi accedere alle notifiche per vedere i set di controllo che ti sono stati delegati per la revisione.

Per accedere alle notifiche

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione sinistro, seleziona Notifiche. In alternativa, nella barra flash blu nella parte superiore della pagina, scegli Visualizza notifica per aprire la pagina delle 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:
 - Data: la data in cui il set di controlli 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 controlli: 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 controlli.
 - Descrizione: le istruzioni di revisione fornite dal proprietario 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 fase di revisione.

5. Consulta le informazioni sul controllo nelle schede Cartella di prove, Origine dati, Commenti e Changelog. Per ulteriori informazioni su ciascuna di queste schede e su come interpretare i dati in esse contenuti, consulta [Esaminare i controlli in una valutazione](#).

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. Questo riepilogo include anche il numero totale di problemi di controllo di conformità segnalati direttamente da AWS Security Hub o da entrambi. AWS Config Per istruzioni su come interpretare i dati in questa pagina, consulta la sezione [Revisione delle cartelle di prove](#).
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 istruzioni su come interpretare i dati in una pagina sui dettagli delle prove, consulta la sezione [Revisione delle cartelle di prove](#).

Fase 3. Carica le prove manuali (facoltativo)

Sebbene raccolga AWS Audit Manager automaticamente le prove per molti controlli, in alcuni casi potrebbe essere necessario fornire prove aggiuntive. In questi casi, puoi caricare manualmente le prove che ti aiutano a dimostrare la conformità a tale controllo.

Prima di poter caricare prove manuali per la valutazione, devi prima inserirle in un bucket S3. Per istruzioni sul caricamento, consulta [Creazione di un bucket](#) e [Caricamento degli oggetti](#) nella Guida per l'utente di Amazon Simple Storage.

Important

Ogni AWS account può caricare manualmente solo fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera fa sì che eventuali caricamenti

manuali aggiuntivi non rientrino in tale controllo. Se devi caricare una grande quantità di prove manuali su un unico controllo, caricale in batch nell'arco di diversi giorni.

Caricare prove manuali per un controllo

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Dalla pagina Notifiche puoi visualizzare l'elenco dei set di controlli che ti sono stati delegati. Identifica il set di controlli per cui desideri aggiungere prove e scegli il nome della valutazione correlata per aprire la pagina dei dettagli della valutazione.
3. Scegli la scheda Controlli, scorri verso il basso fino a Set di controlli, quindi seleziona il nome di un controllo per aprirlo.
4. Scegli la scheda Cartelle di prove, quindi scegli Carica prove manuali.
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 per caricare le prove manuali.

Note

Quando uno stato di controllo è nello stato inattivo, non puoi caricare prove manuali relative a quel controllo. Per caricare prove manuali, devi prima modificare lo stato del controllo impostandolo su In fase di revisione o Revisionato. Per istruzioni su come modificare lo stato di un controllo, consulta [Fase 5: contrassegna un controllo come revisionato \(facoltativo\)](#).

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 commento 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.

A questo punto come si può procedere?

Puoi continuare con ulteriori informazioni sui concetti introdotti in questo tutorial. Di seguito sono riportate alcune risorse consigliate:

- [Revisione di una valutazione](#) - Presenta la pagina di valutazione in cui puoi esplorare i diversi componenti di una valutazione in AWS Audit Manager.
- [Esamina i controlli in una valutazione](#) e [Rivedi le prove in una valutazione](#): fornisce definizioni dei dati per aiutarti a interpretare i controlli e le prove per ogni valutazione.
- [concetti e terminologia AWS Audit Manager](#) - Fornisce le definizioni dei concetti e della terminologia utilizzati in Audit Manager.

Utilizzo del pannello di controllo Audit Manager

Con il pannello di controllo Audit Manager, 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 Audit Manager. 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 prestazione (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 Audit Manager 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](#)
- [Elementi del pannello di controllo](#)
- [Cosa devo fare dopo?](#)
- [Risoluzione dei problemi](#)

Concetti e terminologia del pannello di controllo

Questa sezione descrive cose importanti da sapere sul pannello di controllo di Audit Manager 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 le persone possono visualizzare le metriche e gli aggregati di 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

Audit Manager 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 evidenze relative alla 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, Audit Manager 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, Audit Manager 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 tali servizi non sono stati abilitati. Questo vale anche se il controllo utilizza un tipo di origine dati che non supporta i controlli di conformità, come prove manuali, chiamate API AWS 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 Esito positivo 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. Audit Manager 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.

Audit Manager classifica i controlli nei seguenti domini di controllo.

Nome del dominio di controllo	Descrizione di cosa regolano questi controlli
Continuità aziendale e pianificazione delle emergenze	Come stabilire processi che proteggano le operazioni aziendali critiche dagli effetti di gravi interruzioni di sistema e di rete.
Gestione delle modifiche	Come testare, approvare, implementare e documentare le modifiche alla propria infrastruttura cloud.
Sicurezza e privacy dei dati	Come proteggere la privacy, la disponibilità e l'integrità dei dati.
Sviluppo e gestione della configurazione	Come mantenere l'infrastruttura cloud nello stato desiderato e coerente.

Nome del dominio di controllo	Descrizione di cosa regolano questi controlli
Governance e supervisione	Come allineare l'uso del cloud computing agli obblighi legali, normativi ed etici.
Identity and Access Management	Come garantire che gli utenti giusti abbiano l'accesso appropriato alle risorse tecnologiche.
Gestione degli incidenti	Come stabilire responsabilità e procedure che garantiscano una risposta rapida ed efficace agli incidenti di sicurezza.
Registrazione e monitoraggio	Come esaminare l'attività degli utenti alla ricerca di indizi che dimostrino il tentativo di esecuzione o l'esecuzione di attività non autorizzate.
Gestione di rete	Come amministrare e gestire la rete di dati utilizzando un sistema di gestione di rete.
Gestione del personale	Come valutare e gestire i rischi per la sicurezza del personale a livello organizzativo.
Sicurezza fisica	Come rilevare e prevenire i problemi di sicurezza fisica nelle proprie strutture.
Gestione del rischio	Come valutare i rischi e le perdite potenziali e come ridurre o eliminare tali minacce.
Gestione della catena di fornitura	Come identificare, valutare e mitigare i rischi associati ai prodotti, ai fornitori e alle catene di fornitura IT.
Gestione dei dispositivi utente	Come ridurre il rischio che l'hardware IT dei dipendenti venga perso, danneggiato o compromesso.
Gestione della vulnerabilità	Come definire, valutare e porre rimedio a tutte le vulnerabilità note delle risorse all'interno della propria infrastruttura cloud.

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 Audit Manager 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 Audit Manager 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](#)
- [Snapshot giornaliero](#)
- [Controlli con prove non conformi raggruppati per dominio di controllo](#)

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.

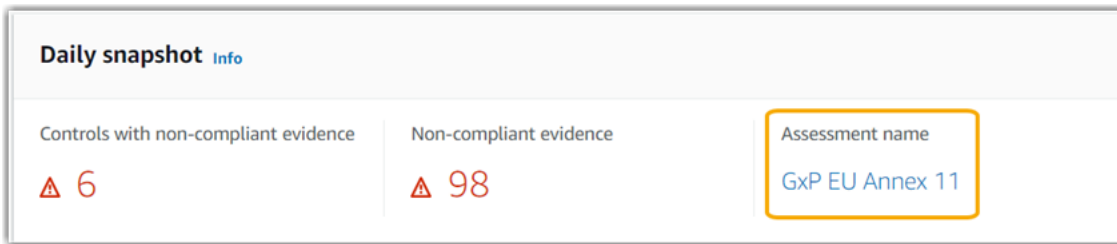
L'istantanea giornaliera riflette i dati più recenti raccolti nella data riportata nella parte superiore del pannello di controllo. La data e l'ora sulla dashboard sono rappresentate in formato UTC. È importante comprendere che questi numeri sono conteggi giornalieri basati su questo timestamp. Ad oggi 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 elementi probatori relativi alla verifica di conformità con una conclusione di non conformità.
3. Valutazioni attive: il numero totale delle valutazioni attive. Scegli questo numero per visualizzare i link a queste valutazioni.

Metric	Value
Controls with non-compliant evidence	220
Non-compliant evidence	658
Active assessments	4

I dati delle istantanee giornalieri 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.

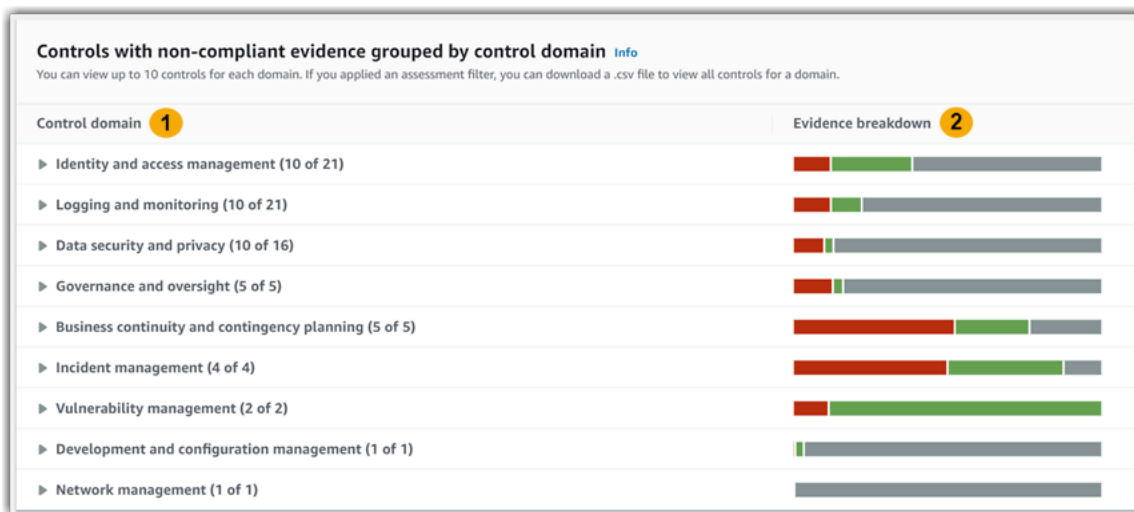


Controlli con prove non conformi raggruppati per dominio di controllo

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.

Control domain	Evidence breakdown	CSV
▼ Identity and access management (4 of 4)		Download
CC6.2 Prior to issuing system credentials and granting system access, the entity registers an...		
CC6.1 The entity implements logical access security software, infrastructure, and architectur...		
CC6.6 The entity implements logical access security measures to protect against threats fro...		
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and o...		

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	AssessmentName	Controllid	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefghijkl-1234-bcde-5678-cdefghijklm	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.

Control domain	Evidence breakdown	CSV
▼ Identity and access management (4 of 4)		Download
CC6.2 Prior to issuing system credentials and granting system access, the entity registers an...		
CC6.1 The entity implements logical access security software, infrastructure, and architectur...		
CC6.6 The entity implements logical access security measures to protect against threats fro...		
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and o...		

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 di controllo: in questa pagina, la [scheda delle cartelle delle prove](#) elenca le cartelle giornaliere delle prove raccolte da Audit Manager per quel controllo. Per maggiori dettagli, scegli una cartella.

2. Cartella delle prove: successivamente, puoi esaminare un [riepilogo della cartella](#) e un [elenco delle prove](#) in essa contenute. Per maggiori dettagli, scegli un singolo elemento di prova.
3. Prove individuali - Infine, puoi esplorare [i dettagli delle singole prove](#). Ciò include tutti gli attributi e i dati relativi alle risorse applicabili alle prove. Questo è il livello più granulare di dati probatori.

Cosa devo fare dopo?

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 di non conformità](#).
- 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, è possibile [modificare la valutazione inattiva](#).

Risoluzione dei problemi

Per trovare risposte a domande e problemi comuni, vedi [Risoluzione dei problemi relativi alla dashboard](#) nella sezione Risoluzione dei problemi di questa guida.

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 dei servizi Account AWS e dei servizi per i quali si desidera raccogliere prove.

È possibile creare una valutazione da qualsiasi framework. In alternativa, è possibile utilizzare un [framework standard](#) fornito da Gestione audit. 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. Per contro, i framework personalizzati contengono controlli che è possibile personalizzare e raggruppare in base ai requisiti di audit interno. Per ulteriori informazioni sulle differenze tra framework standard e personalizzati, consulta [Framework](#) nella sezione Concetti e terminologia di questa guida.

La creazione di una valutazione avvia la raccolta continua di prove. Al momento dell'audit, tu o un delegato di tua scelta potete esaminare le prove raccolte e aggiungerle a un report di valutazione.

Note

AWS Audit Manager aiuta a raccogliere prove pertinenti per verificare la conformità a specifici standard e regolamenti di conformità. Non viene tuttavia 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.

Argomenti

- [Creazione di una valutazione](#)
- [Accedere alle valutazioni in AWS Audit Manager](#)
- [Modifica di una valutazione](#)
- [Revisione di una valutazione](#)
- [Revisione dei controlli in una valutazione](#)
- [Revisione dei controlli in una valutazione](#)
- [Aggiungere prove manuali in AWS Audit Manager](#)

- [Generazione di un report di valutazione](#)
- [Modifica dello stato di una valutazione in inattiva](#)
- [Eliminazione di una valutazione](#)

Creazione di una valutazione

Questo argomento si basa sul tutorial [Guida introduttiva: creazione di una valutazione](#). Contiene istruzioni dettagliate su come creare una valutazione da un framework. Segui questi passaggi per creare una valutazione e avviare la raccolta continua di prove.

Attività

- [Fase 1: specificare i dettagli della valutazione](#)
- [Fase 2: Specificare Account AWS l'ambito](#)
- [Fase 3: Specificare Servizi AWS l'ambito](#)
- [Fase 4: specificare i proprietari dell'audit](#)
- [Passaggio 5: revisione e creazione](#)
- [Cosa posso fare dopo?](#)

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 Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione selezionare Valutazioni, quindi scegli Crea valutazione.
 - In alternativa, nel riquadro di navigazione scegliere Guida introduttiva, quindi Crea valutazione.
3. Nella sezione Nome valutazione, inserisci un nome per la valutazione.
4. (Facoltativo) Nella sezione Descrizione della valutazione, inserisci una descrizione per la valutazione.
5. Nella sezione Destinazione dei report di valutazione, scegli il bucket Amazon S3 in cui desideri salvare i report di valutazione.

Tip

La destinazione predefinita del report di valutazione si basa sulle impostazioni della Gestione Audit. Per ulteriori informazioni, vedere le impostazioni di [AWS Audit Manager](#), [Destinazione del report di valutazione](#). Se preferisci, puoi creare e utilizzare più bucket S3 per aiutarti a organizzare i report di valutazione.

- Nella sezione Frameworks, 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. Si apre la pagina di riepilogo del framework. In questa pagina, puoi rivedere il contenuto di quel framework. Ciò include i controlli e le origini dati del framework.

- Nella sezione 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. Per ulteriori informazioni sui tag in Gestione Audit, consulta [Tagging delle risorse AWS Audit Manager](#).
- 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 scelto. Quindi, convalida questi requisiti in base ai parametri delle regole correnti AWS Config. 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 di creare 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-policy](#) regola 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 Gestione audit possono essere eseguite su più account, con le prove raccolte consolidate in un account amministratore delegato. Per abilitare Organizations in Gestione audit, vedere [Abilita 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 questione, puoi [modificare 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 Servizi AWS l'ambito

Il framework selezionato in precedenza definisce gli elementi per Servizi AWS i quali Audit Manager monitora e raccoglie le prove. Se un elenco Servizio AWS non è selezionato o è selezionato ma non l'hai abilitato nel tuo ambiente, Audit Manager non raccoglie prove dalle risorse relative a quel servizio.

È possibile specificare l' Servizi AWS ambito come segue.

Per le valutazioni create da framework standard

Quando si utilizza la console Audit Manager per creare una valutazione da un framework standard, l'elenco degli Servizi AWS ambiti inclusi viene selezionato per impostazione predefinita. L'elenco non può essere modificato. Questo perché Audit Manager mappa e seleziona automaticamente le origini dati e i servizi per te. La selezione viene effettuata in base ai requisiti del framework standard. Se il framework standard selezionato contiene solo controlli manuali, nessuno Servizi AWS rientra nell'ambito della valutazione e non è possibile aggiungere alcun servizio alla valutazione.

Per proseguire, rivedere l'elenco e scegliere Successivo.

Tip

Se è necessario modificare l'elenco dei servizi inclusi nell'ambito, è possibile farlo utilizzando l'[CreateAssessmentAPI](#) fornita da Audit Manager.

In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per le valutazioni create da framework personalizzati

Se hai selezionato un framework personalizzato nel [passaggio 1](#), puoi rivedere e modificare l'elenco di quelli Servizi AWS che rientrano nell'ambito della valutazione. Se il framework personalizzato selezionato contiene solo controlli manuali, Servizi AWS vengono visualizzati tutti ma nessuno è selezionato. È possibile selezionare zero o più servizi da includere nell'ambito della valutazione.

Da specificare Servizi AWS nell'ambito (solo per le valutazioni create da framework personalizzati)

1. Nella sezione Servizi AWS, seleziona i servizi che desideri includere nell'ambito della valutazione. Puoi trovare servizi aggiuntivi utilizzando la barra di ricerca per servizio, categoria o descrizione. Per aggiungere un servizio, seleziona la casella di controllo accanto al nome del servizio. Per rimuovere un servizio, deseleziona la casella di controllo.
2. Al termine della selezione Servizi AWS, scegli Avanti.

Fase 4: specificare i proprietari dell'audit

In questa fase, l'utente 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 colonna Account AWS mostra l'associato Account AWS del proprietario dell'audit.
2. I proprietari dell'audit che hanno una casella di controllo selezionata sono inclusi nella valutazione. Deseleziona 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.

Passaggio 5: 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, puoi interrompere la raccolta delle prove per un controllo specifico [modificando lo stato del controllo](#) e impostandolo su 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.

Cosa posso fare dopo?

Dopo aver creato la valutazione, è possibile ottenere ulteriori informazioni su:

- [Accedere a una valutazione](#)
- [Revisione di una valutazione](#)
- [Modifica di una valutazione](#)
- [Revisione dei controlli in una valutazione](#)
- [Revisione dei controlli in una valutazione](#)
- [Caricamento di prove manuali per una valutazione](#)
- [Deleghe in AWS Audit Manager](#)
- [Generazione di un report di valutazione](#)
- [Modifica dello stato di una valutazione](#)
- [Eliminazione di una valutazione](#)
- [Risoluzione dei problemi di valutazione e raccolta di prove](#)

Accedere alle valutazioni in AWS Audit Manager

Puoi visualizzare tutte le tue valutazioni nella pagina Valutazioni della console Gestione audit. Da qui puoi anche [modificare una valutazione](#), [eliminare una valutazione](#) o [creare una valutazione](#).

Puoi anche visualizzare le tue valutazioni utilizzando l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare le tue valutazioni (console)

1. Apri la console 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 valutazioni attive e passate. È inoltre possibile utilizzare la barra di ricerca per cercare una valutazione.
3. Scegli un nome per la valutazione per aprire una pagina di riepilogo, in cui è possibile visualizzare i dettagli della valutazione.

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 (API)

Per visualizzare le valutazioni in Audit Manager, utilizzare l'[ListAssessments](#) operazione. È possibile utilizzare l'attributo [status](#) per visualizzare le valutazioni attive o inattive.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Guida della AWS Audit Manager Documentazione di riferimento dell'API. Ciò include informazioni su come utilizzare l'operazione e i parametri di `ListAssessments` degli SDK specifici della lingua AWS .

Modifica di una valutazione

È possibile modificare le valutazioni attive in Gestione audit per cambiare informazioni come la descrizione, l'ambito, i proprietari dell'audit e la destinazione del report di valutazione.

Attività

- [Fase 1: modificare i dettagli della valutazione](#)
- [Fase 2: Modifica dell' Account AWS ambito](#)
- [Fase 3: Modifica Servizi AWS nell'ambito](#)
- [Fase 4: modificare i proprietari dell'audit](#)
- [Fase 5: revisione e salvataggio](#)

Fase 1: modificare i dettagli della valutazione

Segui questi passaggi per modificare i dettagli della valutazione.

Per modificare una valutazione

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione, scegli Valutazioni per visualizzare l'elenco corrente delle valutazioni.
3. Seleziona una valutazione e scegli Modifica.
 - In alternativa, puoi aprire la valutazione e quindi scegliere Modifica in alto a destra della pagina.
4. In Modifica i dettagli della valutazione, modifica il nome, la descrizione e la destinazione del report di valutazione.
5. Seleziona Successivo.

Tip

Per modificare i tag di una valutazione, apri la valutazione e scegli [Scheda Tag](#). Qui puoi visualizzare e modificare i tag associati alla valutazione.

Fase 2: Modifica dell' Account AWS ambito

In questa fase, puoi modificare l'elenco degli account inclusi nell'ambito della valutazione.

Gestione audit supporta più account tramite l'integrazione con AWS Organizations. Ciò significa che le valutazioni di Gestione audit possono essere eseguite su più account, con le prove raccolte

consolidate in un account amministratore delegato. Per aggiungere o modificare l'amministratore delegato per Gestione audit, vedere [AWS Audit Manager impostazioni, Amministratore delegato](#).

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 modificare Account AWS nell'ambito

1. In Modifica Account AWS nell'ambito, seleziona AWS account aggiuntivi. Inoltre, è possibile rimuovere gli account eliminandoli dall'elenco.
2. Seleziona Successivo.

Fase 3: Modifica Servizi AWS nell'ambito

Questo passaggio specifica per quali Servizi AWS Audit Manager monitora e raccoglie le prove. Se un elenco Servizio AWS non è selezionato o è selezionato ma non l'hai abilitato nel tuo ambiente, Audit Manager non raccoglie prove dalle risorse relative a quel servizio.

È possibile rivedere e modificare l' Servizi AWS ambito come segue.

Per le valutazioni create da framework standard

Quando si utilizza la console Audit Manager per modificare una valutazione creata da un framework standard, è possibile rivedere l'elenco di Servizi AWS in scope ma non modificare questo elenco. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente, in base alla progettazione del framework standard. Se la valutazione è stata creata utilizzando un framework che contiene solo controlli manuali, non Servizi AWS rientra nell'ambito della valutazione e non è possibile aggiungere alcun servizio.

Per proseguire, rivedere l'elenco e scegliere Successivo.

Tip

Se è necessario modificare l'elenco dei servizi nell'ambito di una valutazione esistente, è possibile farlo utilizzando l'[UpdateAssessmentAPI](#) fornita da Audit Manager.

Per le valutazioni create da framework personalizzati

Se hai creato la valutazione da un framework personalizzato, puoi modificare i Servizi AWS che rientrano nell'ambito della valutazione. È possibile selezionare zero o più servizi da includere nell'ambito della valutazione.

Da modificare Servizi AWS nell'ambito (solo per le valutazioni create da framework personalizzati)

1. In Modifica Servizi AWS nell'ambito, seleziona Altro Servizi AWS se necessario. Inoltre, è possibile rimuovere servizi eliminandoli dall'elenco.
2. Seleziona Successivo.

Fase 4: modificare i proprietari dell'audit

Inoltre, è possibile modificare 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. I loro compiti comprendono la delega dei set di controllo per la revisione e la generazione di report di valutazione. Ti consigliamo di utilizzare la politica. [AWSAuditManagerAdministratorAccess](#)

Per modificare i proprietari dell'audit

1. Seleziona nuovi proprietari dell'audit da aggiungere alla valutazione. Per rimuovere i proprietari dell'audit, eliminali dall'elenco.
2. Seleziona Successivo.

Fase 5: revisione e salvataggio

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.

Note

Dopo aver completato le modifiche, le modifiche alla valutazione entreranno in vigore alle 00:00 UTC del giorno successivo.

Revisione di una valutazione

Dopo aver creato le valutazioni in Gestione audit, puoi aprirle e rivederle in qualsiasi momento.

Per aprire e rivedere una valutazione

1. Apri la console 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.

Quando apri una valutazione, viene visualizzata una pagina di riepilogo che contiene diverse sezioni. Le sezioni di questa pagina e il relativo contenuto sono descritti come segue.

Sezioni della pagina di valutazione

- [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](#)

Dettagli della valutazione

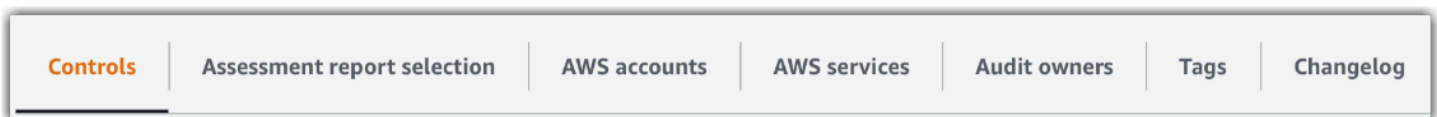
La sezione Dettagli della valutazione fornisce una panoramica della valutazione.

Assessment details			
Name FedRampAssessment 1	Assessment report selection 4 0	AWS accounts 7 1	Assessment status 10 ☑ Active
Description 2 -	Total evidence 5 0	AWS services 8 11	Date created 11 November 21, 2020, 1:16 AM UTC
Compliance type 3 FedRAMP	Assessment reports destination 6 s3://[redacted]	Audit owners 9 1	Last updated 12 November 21, 2020, 1:17 AM UTC

Includi le seguenti informazioni:

1. Nome: il nome che hai fornito per la valutazione.
2. Descrizione: la descrizione facoltativa che hai fornito per la valutazione.
3. Tipo di conformità: lo standard o il regolamento di conformità supportato dalla valutazione.
4. Selezione del report di valutazione: il numero di elementi probatori che l'utente sceglie di includere nel report di valutazione.
5. Evidenza totale: il numero totale di elementi probatori raccolti per questa valutazione.
6. Destinazione dei report di valutazione: il bucket Amazon S3 in cui Gestione audit salva il report di valutazione.
7. Account AWS— Il numero di quelli Account AWS che rientrano nell'ambito di questa valutazione.
8. Servizi AWS— Il numero di quelli Servizi AWS che rientrano nell'ambito di questa valutazione.
9. Titolari dell'audit: il numero di titolari dell'audit per questa valutazione.
10. Lo stato della valutazione: lo stato della valutazione.
 - Attivo: indica che la valutazione sta attualmente raccogliendo prove. Le valutazioni appena create hanno questo stato.
 - Inattivo: indica che la valutazione non sta più raccogliendo prove. Per ulteriori informazioni sulle valutazioni inattive, consulta [Modifica dello stato di una valutazione in inattiva](#).
11. Data di creazione: la data di creazione della valutazione.
12. Ultimo aggiornamento: la data dell'ultima modifica della valutazione.

Scheda Controlli



La scheda Controlli mostra un riepilogo dei controlli della valutazione, insieme a un elenco completo di tali controlli. Ogni valutazione può contenere più set di controlli e ogni set di controlli contiene più controlli. I controlli e i set di controlli sono organizzati in modo da corrispondere al layout definito nello standard o nel regolamento di conformità associato.

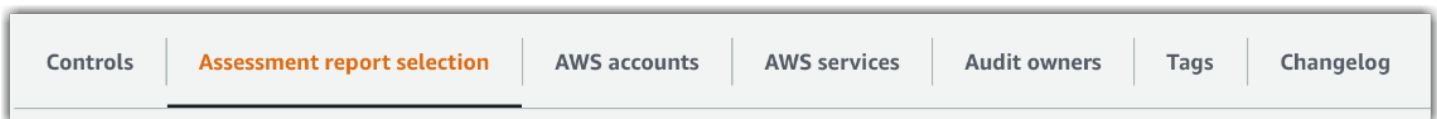
In Riepilogo dello stato del controllo, puoi visualizzare un riepilogo dei controlli per questa valutazione. La tabella di riepilogo include le seguenti informazioni:

- **Controlli totali:** il numero totale di controlli inclusi in questa valutazione.
- **Revisionato:** il numero di controlli che sono stati esaminati da un titolare o delegato dell'audit.
- **In fase di revisione:** il numero di controlli attualmente in fase di revisione.
- **Inattivo:** il numero di controlli che non raccolgono più prove attivamente.

Nella tabella Set di controlli, viene visualizzato un elenco di controlli raggruppati per set di controlli. È possibile espandere o comprimere i controlli in ogni set di controlli. È inoltre possibile eseguire la ricerca in base al nome del controllo se si desidera cercare un controllo particolare. Le seguenti colonne di dati vengono visualizzate nella tabella Controlli raggruppati per set di controlli:

- **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 sono ancora in fase di raccolta per questo controllo ed è possibile caricare 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 per questo controllo ed è possibile caricare prove manuali.
 - **Inattivo** indica che la raccolta automatica delle prove è stata interrotta per questo controllo. Non è più possibile caricare prove manuali.
- **Delegato a:** il revisore di questo controllo, se è stato assegnato a un delegato per la revisione.
- **Evidenza totale:** il numero totale di elementi probatori raccolti per questo controllo.

Scheda di selezione del report di valutazione



Questa scheda mostra l'elenco delle prove da includere nel report di valutazione, raggruppate per cartelle di prove. Queste cartelle di prove sono organizzate e denominate in base alla data di creazione. Puoi sfogliare queste cartelle e selezionare le prove che desideri includere nel report di valutazione. È inoltre possibile utilizzare la barra di ricerca per effettuare la ricerca in base al nome della cartella delle prove o al nome del controllo. Il numero totale di elementi probatori aggiunti al report di valutazione è riepilogato nella sezione Dettagli della valutazione nella parte superiore della pagina.

La tabella di Selezione del report di valutazione mostra un elenco di cartelle di prove con i seguenti dati:

- 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 report di valutazione.
- Nome del controllo: il nome del controllo associato a questa cartella delle prove.

Per informazioni sull'aggiunta di prove a un report di valutazione, consultare [Generazione di un report di valutazione](#).

Account AWS scheda



Questa scheda mostra l'elenco di quelli Account AWS che rientrano nell'ambito della valutazione. Il numero totale di account è riepilogato nella sezione Dettagli della valutazione nella parte superiore della pagina.

La tabella Account AWS mostra un elenco di account con i seguenti dati:

- ID account: l'ID dell' Account AWS.
- Nome account: il nome dell' Account AWS.
- E-mail: l'indirizzo e-mail associato con l' Account AWS.

Servizi AWS scheda



Questa scheda mostra l'elenco di quelli Servizi AWS che rientrano nell'ambito della valutazione. In altre parole, questi sono gli elementi su Servizi AWS cui la valutazione raccoglie le prove.

Il numero totale di servizi è riepilogato nella sezione Dettagli della valutazione nella parte superiore della pagina.

La tabella Servizi AWS mostra un elenco di servizi con i seguenti dati:

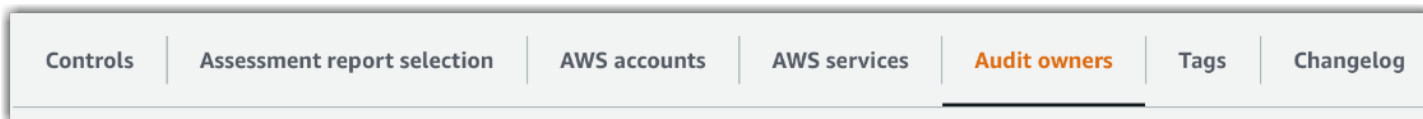
- Servizio AWS: nome della Servizio AWS.
- Categoria: la categoria del servizio, ad esempio elaborazione o database.

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 dall'[origine dati](#) di un controllo. 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, consulta [Qual è la differenza tra un servizio in ambito e un tipo di origine dati?](#) in questa guida.

Note

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. Se è necessario modificare l'elenco dei servizi inclusi nell'ambito, è possibile utilizzare l'[UpdateAssessmentAPI](#).

Scheda titolari audit

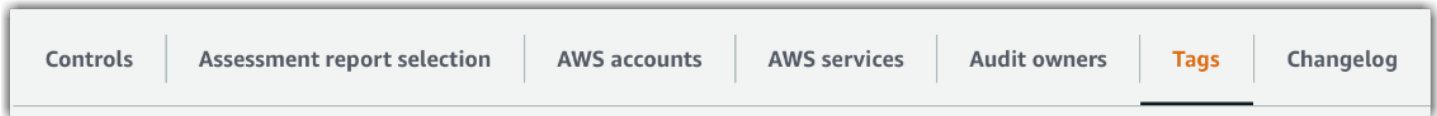


Questa scheda mostra i titolari dell'audit per la valutazione. Il numero totale di titolari dell'audit è riepilogato anche nella sezione Dettagli della valutazione nella parte superiore della pagina.

La tabella Titolari audit mostra un elenco di account con i seguenti dati:

- Titolare audit: il nome del titolare dell'audit.
- Account AWS: l'indirizzo email associato al titolare dell'audit.

Scheda Tag



Questa scheda mostra l'elenco dei tag ereditati dal framework utilizzati per creare questa valutazione. Il numero totale di servizi è riepilogato nella sezione Dettagli della valutazione nella parte superiore della pagina.

La tabella Tag mostra un elenco di servizi con i seguenti dati:

- Chiave: la chiave del tag, ad esempio, uno standard di conformità, un regolamento o una categoria.
- Valore: il valore del tag.

Per ulteriori informazioni sui tag in Gestione Audit, consulta [Tagging delle risorse AWS Audit Manager](#).

Scheda Changelog



Questa scheda mostra un elenco delle attività degli utenti relative alla valutazione.

La tabella Changelog mostra un elenco di account con i seguenti dati:

- Data: la data dell'attività.
- Utente: l'utente che ha eseguito l'azione.
- Azione: l'azione che si è verificata, ad esempio la creazione di una valutazione.
- Tipo: il tipo di oggetto modificato, ad esempio una valutazione.
- Risorsa: la risorsa interessata dalla modifica, ad esempio il framework da cui è stata creata la valutazione.

Revisione dei controlli in una valutazione

I controlli in Gestione audit ti aiutano a soddisfare gli standard e le normative di conformità comuni e unici nei tuoi audit. Puoi aprire e rivedere i controlli nella tua valutazione Gestione audit in qualsiasi momento.

Per aprire una pagina di riepilogo del controllo

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione scegliere Valutazioni, quindi scegliere 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.

Quando apri un controllo viene visualizzata una pagina di riepilogo che contiene diverse sezioni. Le sezioni di questa pagina e il relativo contenuto sono descritti come segue.

Sezioni della pagina di controllo

- [Dettagli del controllo](#)
- [Aggiorna lo stato del controllo](#)
- [Scheda Cartelle delle prove](#)
- [Scheda Origine dati](#)
- [Scheda Commenti](#)
- [Scheda Changelog](#)

Dettagli del controllo

La sezione Dettagli controllo fornisce una panoramica del controllo.

Include le seguenti informazioni:

1. Nome del controllo: il nome assegnato a questo controllo.
2. Descrizione del controllo: la descrizione fornita per questo controllo.
3. Informazioni sui test: le procedure di test consigliate per questo controllo.

4. Piano d'azione: le azioni consigliate da eseguire se il controllo non viene rispettato.

Aggiorna lo stato del controllo

Nella sezione **Aggiorna lo stato del controllo** della pagina, puoi rivedere e aggiornare lo stato del controllo di valutazione.

Sono disponibili i seguenti stati:

- **In fase di revisione:** indica che questo controllo non è ancora stato esaminato. Le prove sono ancora in fase di raccolta per questo controllo ed è possibile caricare 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 caricare prove manuali.
- **Inattivo:** indica che la raccolta automatica delle prove è stata interrotta per questo controllo. Non è più possibile caricare prove manuali.

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.

Scheda Cartelle delle prove

La scheda **Cartelle delle prove** elenca le prove raccolte automaticamente per questo controllo. È organizzata in cartelle su base giornaliera.

La tabella **Cartelle delle prove** mostra un elenco di cartelle con i seguenti dati:

- **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 rilevati 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 non lo hai o non lo hai

AWS Config abilitato AWS Security Hub oppure che le prove provengono da un tipo di origine dati diverso.

- Prove totali: il numero totale di elementi probatori all'interno della cartella.
- Selezione del report di valutazione: il numero di elementi probatori all'interno della cartella inclusi nel report di valutazione.

Dalla scheda Cartelle delle prove, puoi eseguire le seguenti azioni:

- Esamina le singole prove: scegli una [cartella delle prove](#) per aprirla. Dalla pagina di riepilogo della cartella delle prove, puoi quindi scegliere le [singole prove](#) che desideri esaminare.
- Aggiungi prove manuali: per ulteriori informazioni, consulta [Aggiungere prove manuali in AWS Audit Manager](#).
- Aggiungi prove a un report di valutazione: per informazioni consultare [Generazione di un report di valutazione](#).

Scheda Origine dati

In questa scheda vengono visualizzate le informazioni sulle origini dati per il controllo. Include le seguenti informazioni:

- Nome dell'origine dati: si applica solo ai controlli personalizzati. Si riferisce al nome descrittivo che hai assegnato a ciascuna origine dati. Puoi usare questo nome per distinguere tra più origine dati che rientrano nello stesso tipo di origine dati
- Tipo di origine dati: specifica da dove provengono i dati relativi alle prove.
 - Se Audit Manager raccoglie le prove, l'origine dati può essere di quattro tipi: AWS Security Hub, AWS Config, AWS CloudTrail, o AWS chiamate API.
 - Se carichi le tue prove, il tipo di origine dati è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale.
- Mappatura: questo è l'attributo di mappatura utilizzato per identificare e recuperare i dati da una origine dati automatizzata.
 - Se il tipo di origine dati è AWS Config, la mappatura è il nome di una AWS Config regola specifica (ad esempio, EC2_INSTANCE_MANAGED_BY_SSM). Audit Manager utilizza questa mappatura per riportare il risultato del controllo delle regole direttamente da AWS Config.
 - Se il tipo di origine dati è AWS Security Hub, la mappatura è il nome di un controllo specifico del Security Hub (ad esempio, 1.1 - Avoid the use of the "root" account). Audit

Manager utilizza questa mappatura per riportare il risultato del controllo di sicurezza direttamente dal Security Hub.

- Se il tipo di origine dati sono chiamate AWS API, la mappatura è il nome di una chiamata API specifica (ad esempio, `ec2_DescribeSecurityGroups`). Audit Manager utilizza questa mappatura per raccogliere la risposta dell'API.
- Se il tipo di origine dati è AWS CloudTrail, la mappatura è il nome di un CloudTrail evento specifico (ad esempio, `CreateAccessKey`). Audit Manager utilizza questa mappatura per raccogliere l'attività utente correlata dai CloudTrail registri.
- Frequenza: la frequenza della raccolta delle prove da questa origine dati. La frequenza varia a seconda dell'origine dati. Per ulteriori informazioni, scegli il valore nella colonna o consulta [Frequenza di raccolta delle prove](#).

Scheda Commenti

Nella scheda Commenti, puoi aggiungere un commento relativo al controllo e alle relative prove. Inoltre, viene visualizzato 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

La scheda Changelog mostra un elenco delle attività dell'utente relative al controllo. 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 Changelog, una tabella mostra le seguenti colonne di dati:

- Data: la data e l'ora dell'attività, rappresentate in formato UTC (Coordinated Universal Time).
- Utente: l'utente o il ruolo che ha eseguito l'attività.
- Azione: una descrizione dell'attività.
- Tipo: l'attributo associato che descrive ulteriormente l'attività.

- **Risorsa:** la risorsa correlata, se applicabile.

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

Revisione dei controlli in una valutazione

Ogni valutazione attiva in Gestione audit raccoglie automaticamente prove da una serie di origini dati. Per ulteriori informazioni, consulta [Come AWS Audit Manager raccoglie le prove](#). Puoi aprire e rivedere i controlli nella tua valutazione Gestione audit in qualsiasi momento.

Per aprire prove a sostegno di un controllo

1. Apri la console 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. Per la pagina di valutazione, scegli la scheda Controlli, scorri verso il basso fino alla tabella Controlli, quindi seleziona il nome di un controllo per aprirlo.
4. Dalla pagina del controllo, scegli la scheda Cartelle di prove. Nella tabella Cartelle di prove, viene visualizzato un elenco di tutte le cartelle di 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.
5. Scegli il nome di una cartella di prove per aprirla.

Da qui, ora puoi esaminare le cartelle delle prove a tale scopo e approfondire ulteriormente per esaminare i singoli elementi di prova, se necessario.

Argomenti

- [Revisione delle cartelle delle prove](#)
- [Revisione delle prove individuali](#)

Revisione delle cartelle delle prove

Quando apri una cartella delle prove, viene visualizzata una pagina di riepilogo della cartella delle prove che contiene due sezioni: una sezione Riepilogo e una tabella Prove. Queste sezioni e il relativo contenuto sono descritti come segue.

- [Sintesi della cartella Prove](#)
- [Tabella delle prove](#)

Sintesi della cartella Prove

La sezione Riepilogo della pagina fornisce una panoramica di alto livello delle prove contenute nella cartella delle prove.

Summary			
Evidence folder details			
Date 1 8/10/2020, 00:00 UTC - 23:59 UTC	Added to assessment report 3 0	Evidence by type	
Control name 2 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating ...	Total evidence 4 5	User Activity 6 1	Compliance check 9 2
Resources 5 8		Configuration data 7 1	Compliance check status 10 <u>1 issue found</u>
		Manual 8 1	

Include le seguenti informazioni:

1. Data: l'ora e la data in cui è stata creata la cartella delle prove, rappresentate in formato UTC (Coordinated Universal Time).
2. Nome del controllo: il nome del controllo associato alla cartella delle prove.
3. Aggiunto al report di valutazione: il numero di elementi probatori che sono stati inclusi manualmente nel report di valutazione.

4. Prove totali: il numero totale di elementi probatori nella cartella delle prove.
5. Risorse: il numero totale di AWS risorse che sono state valutate durante la generazione delle prove contenute in questa cartella.
6. Attività dell'utente: il numero di elementi probatori che rientrano nella categoria delle attività degli utenti. Queste prove vengono raccolte dai AWS CloudTrail registri.
7. Dati di configurazione: il numero di elementi di prova che rientrano nella categoria dei dati di configurazione. Queste prove vengono raccolte dagli snapshot di configurazione di altri sistemi Servizi AWS come Amazon EC2, Amazon S3 o IAM.
8. Manuale: il numero di elementi probatori che rientrano nella categoria manuale. Queste prove vengono caricate manualmente.
9. Controllo di conformità: il numero di elementi di prova che rientrano nella categoria del controllo di conformità. Queste prove vengono raccolte da o. AWS Config AWS Security Hub
10. Stato del controllo di conformità: il numero totale di problemi segnalati direttamente da AWS Security Hub AWS Config, o entrambi.

Tip

Per ulteriori informazioni sui diversi tipi di prove (attività dell'utente, dati di configurazione, controllo di conformità e manuale), consulta [Prove](#).

Tabella delle prove

La tabella delle prove elenca le singole prove contenute nella cartella delle prove.

Include le seguenti informazioni:

1. Ora: specifica quando sono state raccolte le prove e funge anche da nome delle prove. L'ora è presentata in formato UTC (Universal Time Code, codice orario universale). Scegliendo un orario in questa colonna si apre una [pagina di dettaglio delle prove](#). La pagina è descritta nella sezione seguente.
2. Prove per tipo: la categoria delle prove.
 - Le prove relative al controllo di conformità vengono raccolte da AWS Config o AWS Security Hub.
 - Le prove dell'attività dell'utente vengono raccolte da AWS CloudTrail log.

- Le prove dei dati di configurazione vengono raccolte dagli snapshot di altri servizi, come Amazon EC2, Amazon S3 o IAM.
 - Le prove manuali sono prove che vengono caricate manualmente.
3. Controllo di conformità: lo stato di valutazione delle prove che rientrano nella categoria 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, significa che l'evidenza non è disponibile o è AWS Config abilitata AWS Security Hub oppure che l'evidenza proviene da un tipo di origine dati diverso.
4. Origine dati: l'origine dati da cui vengono raccolte le prove.
5. Nome dell'evento: il nome dell'evento incluso nelle prove.
6. Risorse: il numero di risorse valutate per generare le prove.
7. Selezione del report di valutazione: indica se le prove sono state selezionate manualmente per l'inclusione nel report 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.

Per caricare prove manuali nella cartella delle prove, scegli Carica prove manuali, inserisci l'URI S3 delle prove, quindi scegli Carica. Per maggiori informazioni, consultare [Aggiungi prove manuali in AWS Audit Manager](#).

Per visualizzare i dettagli di ogni singola prova, scegli il nome della prova con collegamento ipertestuale nella colonna Ora. Si apre una pagina dei dettagli delle prove, descritta nella sezione seguente.

Revisione delle prove individuali

Quando si apre una singola prova, viene visualizzata una pagina di dettaglio delle prove che contiene tre sezioni: la sezione Dettagli delle prove, la tabella Attributi e la tabella Risorse incluse. Queste sezioni e il relativo contenuto sono descritti come segue.

- [Dettagli delle prove](#)
- [Attributes](#)

- [Risorse incluse](#)

Dettagli delle prove

La sezione relativa ai dettagli delle prove della pagina mostra una panoramica delle prove.

Evidence detail			
Date and time 1 8/10/20, 18:55:18 UTC	Event source 4 iam.amazonaws.com	Evidence by type 7 User activity	AWS account 11 Account name (#...)
Evidence folder name 2 2020-08-10	Event name 5 UpdateAccountPasswordPolicy	Compliance check 8 Not applicable	IAM ID 12 ...
Control name 3 Ensure IAM password policy requires minimum password length of 20 or greater	Data source 6 AWS CloudTrail	Resources included 9 2	Added to assessment report 13 No
		Attributes 10 4	

Includi le seguenti informazioni:

1. Data e ora: l'ora e la data in cui è stata creata la cartella delle prove, rappresentate in formato UTC (Coordinated Universal Time).
2. Nome della cartella delle prove: il nome della cartella delle prove che contiene le prove.
3. Nome del controllo: il nome del controllo associato alle prove.
4. Origine dell'evento: il nome della risorsa che ha creato l'evento probatorio.
5. Nome dell'evento: il nome dell'evento probatorio.
6. Origine dati: l'origine dati da cui vengono raccolte le prove.
7. Prove per tipo: il tipo delle prove.
 - Le prove relative al controllo della conformità vengono raccolte da AWS Config o AWS Security Hub.
 - Le prove dell'attività dell'utente vengono raccolte da AWS CloudTrail log.
 - Le prove dei dati di configurazione vengono raccolte da snapshot di altri Servizi AWS sistemi come Amazon EC2, Amazon S3 o IAM.
 - Le prove manuali sono prove che vengono caricate manualmente.
8. Controllo di conformità: lo stato di valutazione delle prove che rientrano nella categoria 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, significa che l'evidenza non è disponibile o è AWS Config abilitata AWS Security Hub oppure che l'evidenza proviene da un'altra fonte di dati.

9. Risorse incluse: il numero di risorse valutate per generare le prove.

10 Attributi: il numero totale di attributi utilizzati dall'evento nelle prove.

11 AWS account: il Account AWS luogo da cui sono state raccolte le prove.

12 ID IAM: l'utente o il ruolo pertinente, se applicabile.

13 Aggiunto al report di valutazione: indica se hai scelto di includere le prove nel report di valutazione.

Attributes

La tabella Attributi mostra i nomi e i valori utilizzati dall'evento in questa evidenza. Include le seguenti informazioni:

- Nome dell'attributo: il requisito per le prove, ad esempio allowUsersToChangePassword.
- Valore: il valore dell'attributo, ad esempio true o false.

Risorse incluse

La tabella Risorse incluse mostra l'elenco delle risorse valutate per generare queste prove. Include uno o più campi tra i seguenti:

- ARN: nome della risorsa Amazon (ARN, Amazon Resource Name). Un ARN potrebbe non essere disponibile per tutti i tipi di prove.
- Valore: il valore di quella risorsa, se applicabile.
- JSON: il collegamento per visualizzare il file JSON per quella risorsa.

Aggiungere prove manuali in AWS Audit Manager

Gestione audit può raccogliere automaticamente prove per molti controlli. Tuttavia, alcuni controlli richiedono l'aggiunta manuale delle proprie 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 caricare manualmente le prove. 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 multcloud, 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.

Per ulteriori informazioni sui diversi tipi di prove in Gestione audit, consulta [Prova](#) nella sezione Concetti e terminologia di questa guida.

Come aggiungere prove manuali

Per aggiungere prove manuali a un controllo di valutazione, è possibile utilizzare i metodi indicati di seguito.

Ricorda:

- È possibile utilizzare un solo metodo alla volta per aggiungere prove manuali.
- La dimensione massima supportata per un singolo file di prove manuali è 100 MB.
- [Formati di file supportati per prove manuali](#) Sono elencati più avanti in questa pagina.
- Ciascuno Account AWS può caricare manualmente fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera fa sì che eventuali caricamenti manuali aggiuntivi non rientrino in tale 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 caricare prove manuali, devi prima modificare lo stato del controllo impostandolo su In fase di revisione o Revisionato. Per istruzioni, consulta [Aggiorna lo stato del controllo](#).

Importare un file da Amazon S3

Attenersi alla seguente procedura per importare prove manuali da un bucket S3.

AWS console

Per importare un file da S3 (console)

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro sinistro di navigazione scegli Valutazioni, quindi scegliere il nome della propria valutazione per aprirla.
3. Scegli la scheda Controlli, scorri verso il basso fino a Set di controlli, quindi scegli il nome di un controllo per aprirlo.
4. Nella scheda Cartelle di prove, scegli Aggiungi prove manuali, quindi scegli Importa file da S3.
 - In alternativa, scegli il nome di una cartella delle prove nella scheda Cartelle delle prove per esaminare il riepilogo della cartella delle prove, quindi scegli Aggiungi prove manuali, 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 (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://example-bucket/example-file.extension
```

Audit Manager API

Per importare un file da S3 (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 precedenti per saperne di più nel AWS Audit Manager Riferimento API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Carica un file dal tuo browser

Segui questi passaggi per caricare prove manuali dal tuo browser.

AWS console

Carica un file dal proprio browser (console)

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro sinistro di navigazione scegli Valutazioni, quindi scegliere il nome della propria valutazione per aprirla.
3. Sulla scheda Controlli, scorri verso il basso fino a Set di controlli, quindi scegli il nome di un controllo per aprirlo.

A questo punto sono disponibili tre modi per caricare un file:

- (Opzione 1) Nel banner blu di notifica, scegli Carica prove manuali.
 - (Opzione 2) Nella scheda Cartelle di prove, scegli Aggiungi prove manuali, quindi scegli Carica file dal browser.
 - (Opzione 3) Scegli il nome di una cartella di prove per rivedere un riepilogo di quella cartella, scegli Aggiungi prove manuali, quindi scegli Carica file dal browser.
4. Scegli il file che si desidera caricare.
 5. Scegli Carica.

AWS CLI

Nella procedura seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

Per caricare un file dal proprio browser (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 `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 [Crittografia dei dati](#) impostazioni di Audit Manager, assicurati di includere anche `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 proprio browser (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 [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 precedenti per saperne di più nel AWS Audit Manager Riferimento API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua. AWS

Inserisci una risposta testuale

Segui questi passaggi per inserire una risposta a una domanda di valutazione del rischio e salvarla come prova manuale.

AWS console

Per inserire una risposta testuale (console)

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro sinistro di navigazione scegli Valutazioni, quindi scegliere il nome della propria valutazione per aprirla.
3. Scegli la scheda Controlli, scorri verso il basso fino a Set di controlli, quindi scegli il nome di un controllo per aprirlo.

Da qui sono disponibili tre modi per inserire una risposta testuale:

- (Opzione 1) Nel banner blu di notifica, scegli Inserisci risposta.
 - (Opzione 2) Nella scheda Cartelle di prove, scegli Aggiungi prove manuali, quindi scegli Inserisci risposta tesuale.
 - (Opzione 3) Scegli il nome di una cartella di prove per rivedere un riepilogo di quella cartella, scegli Aggiungi prove manuali, quindi scegli Inserisci risposta testuale.
4. Nella finestra pop-up che appare, inserisci la risposta in formato testo semplice.
 5. Scegli Conferma.

AWS CLI

Nella procedura seguente, sostituisci ciascun *testo segnaposto* con le tue informazioni.

Per inserire una risposta testuale (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 testuale (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, scegli uno dei link precedenti per saperne di più nel AWS Audit Manager Riferimento API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua. AWS

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

Generazione di un report di valutazione

Un report di valutazione riassume la valutazione e fornisce collegamenti a un set organizzato di cartelle che contengono le prove correlate. Per ulteriori informazioni, consulta [Report di valutazione](#).

È possibile scegliere quali prove includere nel report di valutazione prima di generare il report stesso. Le prove appena raccolte non vengono incluse automaticamente in un report di valutazione.

Attività

- [Aggiungere prove a un report di valutazione](#)
- [Rimuovere le prove da un report di valutazione](#)
- [Generazione di un report di valutazione](#)

- [Cosa posso fare dopo?](#)

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 singoli elementi di prova dall'interno di una cartella.

Aggiungere prove a un report di valutazione

1. Apri la console 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 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.
 - 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.
 - 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.

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.

Per rimuovere le prove da un report di valutazione

1. Apri la console 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.
 - 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.
 - 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.

Generazione di un report di valutazione

Dopo aver aggiunto le prove al report di valutazione, puoi generare il report 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.

Tip

Per assicurarti che il report di valutazione venga generato correttamente, consulta il nostro [Suggerimenti di configurazione per la destinazione del rapporto di valutazione](#)

Per generare un report di valutazione

1. Apri la console 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.
 - 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.

Il report di valutazione ha un checksum del file che ne garantisce l'integrità. Puoi convalidarlo con l'operazione [ValidateAssessmentReportIntegrity](#) API fornita da Audit Manager.

Cosa posso fare dopo?

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 l'operazione [ValidateAssessmentReportIntegrity](#) API 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](#).

Modifica dello stato di una valutazione in inattiva

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.

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 una valutazione in inattivo (console)

1. Apri la console 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 (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-status](#) comando 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 (API)

1. Utilizzate l'[ListAssessments](#) operazione per trovare la valutazione che desiderate disattivare e prendete nota dell'ID della valutazione.
2. Utilizzate l'[UpdateAssessmentStatus](#) operazione 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, scegli i 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.

Eliminazione di una valutazione

È possibile eliminare qualsiasi valutazione di Gestione audit che non serve più. 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 (console)

1. Apri la console 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.
 - In alternativa, puoi aprire la valutazione e quindi scegliere Elimina in alto a destra della pagina.

AWS CLI

Per eliminare una valutazione (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 (API)

1. Utilizzate l'[ListAssessments](#) operazione per trovare la valutazione che desiderate eliminare.

Nella risposta, prendere nota dell'ID di valutazione.

- Utilizzate l'[DeleteAssessment](#) operazione e specificate l'[AssessmentID](#) della valutazione che desiderate eliminare.

Per ulteriori informazioni su queste operazioni API, scegli uno dei link precedenti per saperne di più nel [AWS Audit Manager Riferimento API](#). Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK AWS specifici della lingua.

 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.

Deleghe in AWS Audit Manager

I proprietari dell'audit utilizzano AWS Audit Manager per creare valutazioni e raccogliere prove per i controlli elencati 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.

A un livello elevato, 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.

Utilizza le seguenti sezioni di questa guida per saperne di più su come gestire le attività di delega in AWS Audit Manager.

Argomenti

- [Compiti di delega per i proprietari dell'audit](#)
- [Compiti di delega per i delegati](#)

Note

Un account può essere proprietario di un audit o delegato in diverse regioni AWS.

Compiti di delega per i proprietari dell'audit

In qualità di proprietario dell'audit in AWS Audit Manager, potresti aver bisogno dell'assistenza di un esperto in materia per aiutarti a esaminare i controlli e le prove. In questa situazione, puoi delegare un set di controlli per la revisione.

Negli argomenti seguenti viene descritto come gestire le deleghe in AWS Audit Manager.

Compiti di delega

- [Delega di un set di controlli per la revisione](#)
- [Accesso alle deleghe attive e completate](#)
- [Eliminazione delle deleghe attive e completate](#)

Delega di un set di controlli per la revisione

Quando hai bisogno dell'assistenza di un esperto in materia, puoi scegliere l'account AWS per il quale desideri assistenza e quindi delegare un set di controlli affinché venga esaminato.

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 AWS Audit Manager 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 tue deleghe in qualsiasi momento scegliendo Deleghe nel pannello di navigazione sinistro 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 AWS Audit Manager 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 tue deleghe in qualsiasi momento scegliendo Deleghe nel pannello di navigazione sinistro della console AWS Audit Manager.

Quando deleghi un set di controlli per la revisione, il delegato riceve una notifica e può quindi iniziare a esaminare il set di controlli. Questo processo seguito dai delegati è descritto in [Compiti di delega per i delegati](#).

Tip

I delegati possono iscriversi a un argomento SNS per ricevere avvisi e-mail quando viene loro delegata un'attività di revisione. Per ulteriori informazioni su come identificare e iscriversi all'argomento SNS associato a AWS Audit Manager, consulta [Notifiche in AWS Audit Manager](#).

Accesso alle deleghe attive e completate

Puoi accedere a un elenco delle tue deleghe in qualsiasi momento scegliendo Deleghe nel pannello di navigazione sinistro della console AWS Audit Manager. La pagina delle deleghe contiene un elenco delle deleghe attive e completate, con i seguenti dettagli per ciascuna delega:

- Delegato a: l'account AWS a cui hai delegato il set di controlli.
- Data: la data in cui hai delegato il set di controlli.
- Stato: lo stato attuale della delega.
- Valutazione: il nome della valutazione con un collegamento alla pagina dei dettagli della valutazione.
- set di controlli: il nome del set di controlli che è stato delegato per la revisione.

Quando una delega è completata, ricevi una notifica in AWS Audit Manager. Puoi inoltre ricevere commenti con osservazioni dal delegato. La procedura seguente spiega come controllare le notifiche in Audit Manager dopo il completamento di una delega e come visualizzare eventuali commenti che il delegato potrebbe aver lasciato per te.

Per visualizzare una delega completata e verificare la presenza di commenti

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione, seleziona Notifiche. In alternativa, nella barra flash blu nella parte superiore della pagina, scegli Notifiche per aprire la pagina delle notifiche.
3. Consulta la pagina Notifiche, che include una tabella con le seguenti informazioni:
 - Data: la data della notifica.
 - Valutazione: il nome della valutazione associata al set di controlli.
 - set di controlli: il nome del set di controlli.
 - Origine: l'utente o il ruolo del delegato che ti ha inviato il set di controlli completo.
 - Descrizione: osservazioni di alto livello fornite dal delegato.
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. 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.

6. Scegli la scheda Commenti per visualizzare eventuali commenti aggiunti dal delegato per quel particolare controllo.
7. Quando ritieni che la revisione di un set di controlli sia completa, seleziona il set di controlli e scegli Completa revisione del set di controlli.

Important

Audit Manager 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 [scheda Changelog](#) della pagina dei dettagli del controllo. Puoi quindi utilizzare questo timestamp per identificare quali prove aggiungere ai rapporti di valutazione.

Eliminazione delle deleghe attive e completate

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 AWS Audit Manager. Puoi anche eliminare le deleghe completate che non desideri più vengano visualizzate nella pagina delle deleghe.

Per eliminare una delega

1. Apri la console AWS Audit Manager 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.

Compiti di delega per i delegati

Generalmente, i delegati hanno competenze commerciali o tecniche specializzate in diverse aree. Tra queste competenze figurano politiche di conservazione dei dati, piani di formazione, infrastruttura di rete e gestione delle identità. Esse possono aiutare i proprietari degli audit a esaminare le prove raccolte per verificare i controlli che rientrano nella loro area di competenza.

In qualità di delegato, potresti ricevere richieste dai proprietari dell'audit per esaminare le prove associate a un set di controlli. Questa richiesta indica che il proprietario dell'audit ha bisogno dell'assistenza dell'utente per la convalida di tali prove. 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.

Negli argomenti seguenti viene descritto come gestire le deleghe in AWS Audit Manager.

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 Audit Manager, consulta [Politiche consigliate per gli utenti in AWS Audit Manager](#).

Compiti di delega

- [Visualizzazione delle notifiche per le richieste di delega in arrivo](#)
- [Revisione di un set di controlli e le relative prove](#)
- [Aggiungere un commento a un controllo](#)
- [Contrassegnare un controllo come revisionato](#)
- [Invio del set di controlli revisionato al proprietario 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.

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](#).

Per visualizzare le notifiche

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione sinistro, seleziona Notifiche. In alternativa, nella barra flash blu nella parte superiore della schermata, scegli Visualizza notifica per aprire la pagina delle 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:
 - Data: la data in cui il set di controlli è stato delegato.
 - Valutazione: il nome della valutazione associata al set di controlli.
 - set di controlli: il nome del set di controlli.
 - Origine: l'utente o il ruolo che ti ha delegato il set di controlli.
 - Descrizione: le istruzioni di revisione fornite dal proprietario dell'audit.

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.

Revisione di un set di controlli

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione, seleziona Notifiche. In alternativa, nella barra flash blu, scegli Visualizza notifica per aprire la pagina delle notifiche.

3. Dalla pagina Notifiche, viene visualizzato un elenco dei 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 e scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
6. (Facoltativo) Scegli Aggiorna stato del controllo per modificare lo stato del controllo. Durante la revisione, puoi contrassegnare lo stato come In fase di revisione.
7. Consulta le informazioni sul controllo nelle schede Cartella di prove, Origine dati, Commenti e Changelog. Per informazioni su ciascuna di queste schede e su come interpretare queste informazioni, consulta [Esaminare i controlli in una valutazione](#).

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.
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, AWS Config da entrambi. Per istruzioni su come interpretare i dati in questa pagina, consulta la sezione [Revisione delle cartelle di prove](#).
4. Dalla pagina di riepilogo della cartella delle prove, vai alla tabella Prove. Nella colonna Ora, scegli un elemento da aprire. Quindi, esamina i dettagli sulla prova raccolta in quel momento. Per istruzioni su come interpretare i dati in una pagina sui dettagli delle prove, consulta la sezione [Revisione delle cartelle di prove](#).

Tip

Sebbene AWS Audit Manager raccolga automaticamente le prove per molti controlli, in alcuni casi potrebbe essere necessario fornire prove aggiuntive per dimostrare la conformità. In

questi casi puoi caricare manualmente le prove. Per istruzioni, consulta [Caricamento delle prove manuali](#).

Aggiungere un commento a un controllo

Puoi aggiungere commenti per tutti i controlli che esamini. Questi commenti sono visibili al proprietario dell'audit.

Per aggiungere un commento a un controllo

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione sinistro, seleziona Notifiche. In alternativa, nella barra flash blu nella parte superiore della schermata, scegli Visualizza notifica per aprire la pagina delle notifiche.
3. Nella pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. Trova il set di controlli che contiene il controllo per cui desideri lasciare un commento e scegli il nome della valutazione correlata.
4. 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 la scheda Commenti.
6. Nella sezione Invia commenti, inserisci il tuo commento nella casella di testo.
7. Scegli Invia commento per aggiungere il tuo commento. Pertanto, il tuo commento viene visualizzato nella sezione Commenti precedenti della pagina, insieme a qualsiasi altro commento relativo a questo controllo.

Contrassegnare un controllo come revisionato

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.

Per contrassegnare un controllo come revisionato

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione sinistro, seleziona Notifiche. In alternativa, nella barra flash blu nella parte superiore della schermata, scegli Visualizza notifica per aprire la pagina delle notifiche.
3. Nella pagina Notifiche, esamina l'elenco dei set di controlli che ti sono stati delegati. Trova il set di controlli che desideri contrassegnare come revisionato e scegli il nome della valutazione correlata.
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. Scegli il nome di un controllo per aprire la pagina dei dettagli del controllo.
6. Scegli Aggiorna lo stato del controllo e modifica lo stato impostandolo su Revisionato.
7. Nella finestra pop-up che appare, scegli Aggiorna lo stato del controllo per confermare di aver terminato la revisione del controllo.

Invio del set di controlli revisionato al proprietario dell'audit

Dopo aver esaminato i controlli che ti sono stati delegati, invia il set di controlli al proprietario dell'audit. In questo modo il processo di delega viene completato.

Per restituire un set di controlli revisionato al proprietario dell'audit

1. Apri la console AWS Audit Manager 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. Dopo aver inviato il controllo al proprietario dell'audit, i destinatari possono visualizzare tutti i commenti che hai lasciato.

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.

Struttura delle cartelle del report 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 report di valutazione (esempio: `reportName-a1b2c3d4e5f6g7`): una sottocartella in cui è possibile trovare i file `AssessmentReportSummary.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.

Come navigare in un report 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.

Sezioni del report 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](#)
- [Pagina di panoramica](#)
- [Pagina del sommario](#)

- [Pagina di controllo](#)
- [Pagina di riepilogo delle prove](#)
- [Pagina dei dettagli delle prove](#)

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 report: nome del report.
- Descrizione: la descrizione inserita dal titolare dell'audit al momento della generazione del report.
- Data di generazione: la data in cui è stato generato il report. L'ora è presentata in formato UTC (Universal Time Code, codice orario universale).
- Controlli totali inclusi: il numero di controlli inclusi nel report sui quali sono state raccolte prove. Si tratta di un sottoinsieme del numero totale di controlli inclusi nella valutazione.
- Account AWS inclusi: il numero di Account AWS inclusi nel report sui quali sono state raccolte prove. Si tratta di un sottoinsieme del numero totale di Account AWS nella valutazione.
- Selezione del report di valutazione: il numero di elementi probatori selezionati per l'inclusione nel report. Ciò include il numero totale di problemi di controllo della conformità rilevati nel report.

Riepilogo della valutazione

Questa sezione riassume la valutazione a cui si riferisce il report.

- **Nome della valutazione:** il nome della valutazione da cui è stato generato il report.
- **Stato:** lo stato della valutazione al momento in cui è stato generato il report.
- **Regione di valutazione:** la Regione AWS in cui è stata creata la valutazione.
- **Account AWS pertinenti:** l'elenco completo di Account AWS che rientrano nell'ambito della valutazione.
- **Servizi AWS pertinenti:** l'elenco completo di Servizi AWS che rientrano 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 proprietari 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.

- **Set di controllo:** il nome del controllo.
- **Descrizione:** la descrizione del controllo.
- **Set di controlli:** il nome del set di controlli a cui appartiene il controllo.

- Informazioni sui test: le procedure di test consigliate per questo controllo.
- Piano d'azione: le azioni consigliate da eseguire se il controllo non viene rispettato.
- Selezione del report di valutazione: il numero di elementi probatori relativi a questo controllo inclusi nel report 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 manuale. Includono inoltre i primi 10 caratteri del nome del file e la sua estensione (fino a 10 caratteri).

Ad esempio: `00-00-00_manuale_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 AWS CloudTrail da chiamate API 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 informazioni riportate di seguito:

- ID: identificatore univoco per le prove.
- Data di 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 origine dati.
- Nome della valutazione: il nome della valutazione da cui è stato generato il report.
- 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.
- Descrizione del controllo: la descrizione del controllo supportato dalle prove.
- Informazioni sui test: le procedure di test consigliate per il controllo.
- Piano di azione: le azioni consigliate da eseguire se il controllo non viene rispettato.
- Regione AWS: nome della regione associata alla prova.
- IAM ID: l'ARN dell'utente o del ruolo associato alle prove.
- Account AWS: L'ID Account AWS associato alle prove.
- Servizio AWS: nome della Servizio AWS associata alla prova.
- Risorse incluse: le risorse di AWS che sono state valutate per generare le prove. Questo attributo non è applicabile alle prove relative al controllo di conformità di AWS Config. Per questo tipo di prova, puoi trovare tutte le risorse elencate nel [Pagina dei dettagli delle prove](#) delle prove.
- Nome dell'evento: il nome dell'evento probatorio.
- Ora dell'evento: l'ora in cui si è verificato l'evento probatorio.
- Origine dati: dove sono state raccolte o caricate le prove. Il tipo di origine dati può essere sia AWS Config, Centrale di sicurezza, AWSchiamate API, CloudTrail o manuale.
- Prove per tipo: la categoria delle prove
 - Le prove del controllo di conformità vengono raccolte dal AWS Config da Security Hub.
 - Le prove dell'attività degli utenti vengono raccolte dai log di CloudTrail.
 - Le prove dei dati di configurazione vengono raccolte da istantanee di altri Servizi AWS.
 - Le prove manuali sono prove che vengono caricate manualmente.
- 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 AWS CloudTrail da chiamate API 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 dei 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.

Verifica dell'integrità del report 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 report di valutazione, utilizza l'API [ValidateAssessmentReportIntegrity](#) fornita da Gestione audit.

Report di valutazione della risoluzione dei problemi

Per trovare le risposte alle domande e ai problemi più comuni, consulta [Risoluzione dei problemi relativi ai report di valutazione](#) nella sezione Risoluzione dei problemi di questa guida.

Evidence finder

Evidence finder offre un modo efficace per cercare prove in Audit Manager. 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 Audit Manager.

Argomenti

- [Comprendere come funziona evidence finder con CloudTrail Lake](#)
- [Attivazione di evidence finder](#)
- [Risoluzione dei problemi evidence finder](#)
- [Ricerca le prove](#)
- [Visualizzare i risultati in evidence finder](#)
- [Filtro e opzioni di raggruppamento](#)
- [Casi d'uso di esempio](#)

Comprendere come funziona evidence finder con CloudTrail Lake

Evidence finder utilizza la funzionalità di interrogazione e archiviazione di [AWS CloudTrail Lake](#). Prima di iniziare a utilizzare evidence finder, è utile saperne di più su come funziona CloudTrail Lake.

CloudTrail Lake aggrega i dati in un unico archivio di dati degli 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 Audit Manager.

Quando richiedi di abilitare evidence finder, Audit Manager crea un archivio di dati degli eventi per tuo conto. Una volta abilitato evidence finder, tutte le prove future dell'Audit Manager 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 [Aggiornare 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

Il processo di riempimento dei dati, quando questa funzionalità è abilitata, è gratuito se completato entro novembre 2023.

In futuro, quando verranno aggiunte nuove prove all'archivio di dati degli eventi, CloudTrail Lake addebiterà i costi per l'archiviazione e l'ingestione dei dati.

Per le query su CloudTrail Lake, considerare il pagamento 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 [Prezzi di AWS CloudTrail](#).

Attivazione di evidence finder

È possibile abilitare evidence finder dalle impostazioni di Audit Manager. Per istruzioni, vedi [evidence finder](#) nella pagina Impostazioni AWS Audit Manager di questa guida.

Risoluzione dei problemi evidence finder

Per trovare risposte a domande e problemi comuni, vedi [Risoluzione dei problemi relativi a evidence finder](#) nel capitolo Risoluzione dei problemi di questa guida.

Ricerca delle prove

Segui questi passaggi per cercare prove nella console Audit Manager.

Note

Puoi anche utilizzare l'API CloudTrail per interrogare i dati delle prove. Per ulteriori informazioni, consulta [StartQuery](#) in Riferimento sull'API AWS CloudTrail. Se preferisci utilizzare AWS CLI, consulta [Avvia una query](#) nella Guida per l'utente AWS CloudTrail.

In questa pagina

- [Esecuzione di una query di ricerca](#)
- [Interruzione di una query di ricerca](#)
- [Modificare i filtri di ricerca](#)

Esecuzione di una query di ricerca

Segui questi passaggi per eseguire una query di ricerca in evidence finder.

Per ricercare le prove

1. Apri la console di Gestione audit AWS Audit all'[indirizzo https://console.aws.amazon.com/auditmanager/home](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.

▼ Filters and grouping
4 filters applied.

Assessment: PCI DSS V3.2.1

Date range: Last 7 days

Resource compliance [Info](#)
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

Select all

Non-compliant Compliant Inconclusive

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.

i Tip

Per ulteriori informazioni sui filtri e sui raggruppamenti che è possibile utilizzare in questa procedura, consulta [Opzioni di filtro e raggruppamento](#).

Interruzione di una query di ricerca

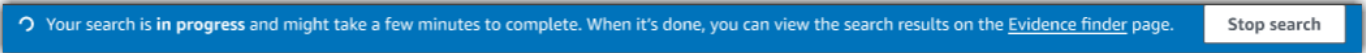
Per interrompere una query di ricerca per qualsiasi motivo, attieniti alla seguente procedura.

i 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.

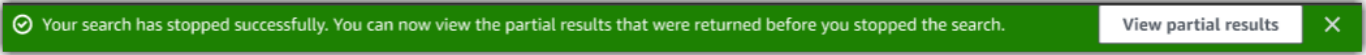
Per interrompere una query di ricerca in corso

1. Nella barra flash di avanzamento blu nella parte superiore della schermata, seleziona **Interrompi la ricerca**.



↻ Your search is in progress and might take a few minutes to complete. When it's done, you can view the search results on the [Evidence finder page](#). **Stop search**

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.



✔ Your search has stopped successfully. You can now view the partial results that were returned before you stopped the search. **View partial results** ✕

Modificare i filtri di ricerca

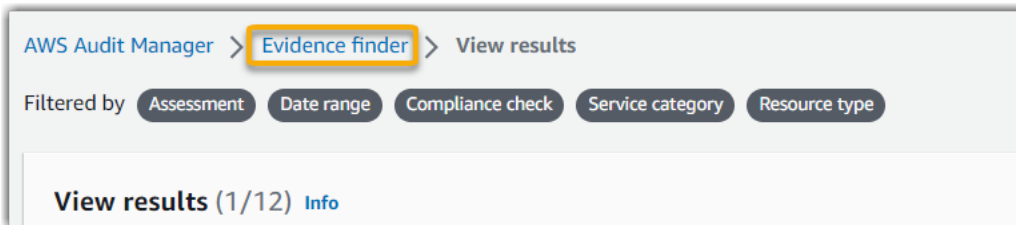
È possibile tornare alla query di ricerca più recente e modificare i filtri in base alle esigenze.

Note

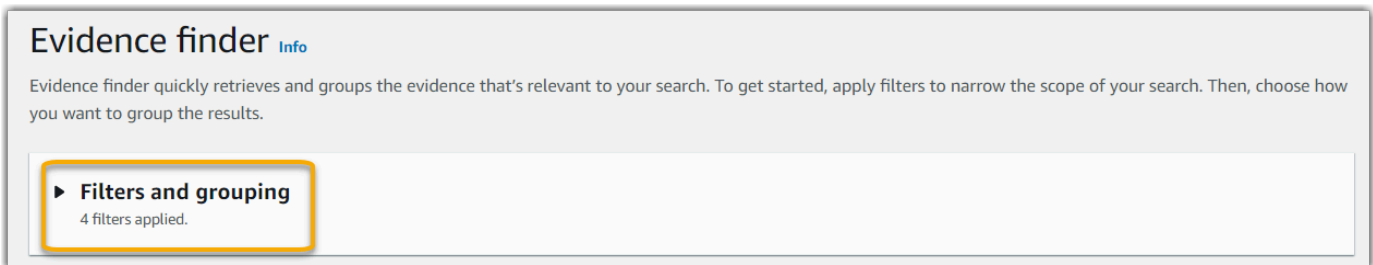
Quando modifichi i filtri e scegli Cerca, viene avviata una nuova query di ricerca.

Modificare 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.



Visualizzare i 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 console CloudTrail 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 console CloudTrail.

In questa pagina

- [Visualizzazione dei risultati raggruppati](#)
- [Visualizzazione dei risultati](#)
 - [Gestisci le preferenze di visualizzazione](#)
 - [Anteprima dei riepiloghi delle risorse](#)
 - [Genera un rapporto di valutazione dai risultati della ricerca](#)
 - [Esportare i risultati della ricerca](#)

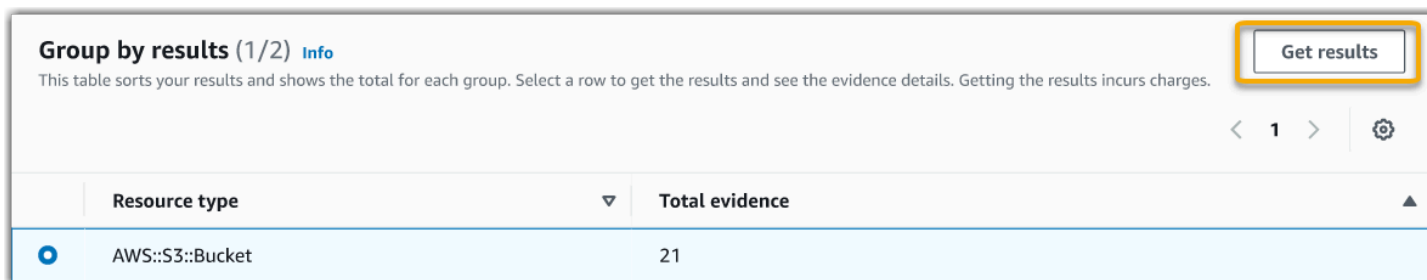
Visualizzazione dei risultati raggruppati

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 il gruppo è stato raggruppato per tipo di risorsa, la tabella mostra un elenco di tipi di risorse AWS. La colonna Prova totale mostra il numero di risultati corrispondenti per ogni tipo di risorsa.



Group by results (1/2) [Info](#)

This table sorts your results and shows the total for each group. Select a row to get the results and see the evidence details. Getting the results incurs charges.

[Get results](#)

< 1 > ⚙

Resource type	Total evidence
<input checked="" type="radio"/> AWS::S3::Bucket	21

Per ottenere i 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.

Visualizzazione dei risultati

La tabella Visualizza risultati mostra i risultati della ricerca. Dal qui, puoi effettuare le operazioni seguenti:

- [Gestisci le preferenze di visualizzazione](#)
- [Anteprima dei riepiloghi delle risorse](#)
- [Genera un rapporto di valutazione dai risultati della ricerca](#)
- [Esportare i risultati della ricerca](#)

Gestisci le preferenze di visualizzazione

Le tue preferenze di visualizzazione controllano ciò che vedi nella pagina dei risultati.

Per gestire le 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:
 - a. Seleziona le colonne visibili della tabella: utilizza l'opzione di attivazione/disattivazione per modificare le colonne visualizzate.
 - b. Dimensioni della pagina: seleziona un pulsante di opzione per specificare il numero di risultati visualizzati su ciascuna pagina.
 - c. Avvolgi testo: seleziona la casella di controllo per disporre lunghe righe di testo per una migliore leggibilità.
3. Per salvare le preferenze, scegli Conferma

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 Audit Manager 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.

Per visualizzare l'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.

The screenshot displays the AWS Audit Manager interface. At the top, there is a table with columns: Evidence, Resource ARN, Resource compliance, and Date and time. The table contains three rows of evidence items. The second row is selected, and a detailed resource summary panel is open below it.

Evidence	Resource ARN	Resource compliance	Date and time
<input type="radio"/> 22615e944-a8b2-4cb0-85e4-d853ea94347b	arn:aws:iam:us-west1:[:policyName]	⚠ Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
<input checked="" type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-[:trail/AWSOrganizationMaster]	✅ Compliant	August 10, 2022, 7:30 (UTC+00:00)
<input type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-[:trail/]	✅ Compliant	August 10, 2022, 7:30 (UTC+00:00)

99615e944-a8b2-4cb0-85e4-d853ea94350d

Resource summary

Resource ARN arn:aws:iam:us-west1:[:policyName]	Data source type AWS Config	Assessment PCI DSS V3.2.1
Resource Type AWS::S3::Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Control domain Identity and access management
Resource compliance ⚠ Non-compliant	Account ID [:]	Control 7.2.1 Confirm that access control systems are in place on all system components.
Date and time August 10, 2022, 7:30 (UTC+00:00)		

Genera un rapporto di valutazione dai risultati della ricerca

Dopo essere soddisfatto dei risultati della ricerca, genera un report di valutazione.

Per generare 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 Audit Manager e [scaricare il report di valutazione](#).

Note

Audit Manager 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 di Evidence finder](#).

Esportare i risultati della ricerca

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 Audit Manager 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, vedi la [struttura dei file di firma di CloudTrail](#) nella Guida per gli sviluppatori AWS CloudTrail. Per determinare se i risultati della query sono stati modificati, eliminati o modificati dopo la consegna, puoi utilizzare la funzionalità di convalida dell'integrità dei risultati della query di CloudTrail. 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 Audit Manager, 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 policy di autorizzazione richiesta per consentire a CloudTrail di scrivere i file di esportazione. Più specificamente, la policy del bucket deve includere un'azione s3:PutObject e l'ARN del bucket, ed elencare CloudTrail come servizio principale. 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, vedi [Risoluzione dei problemi relativi alle esportazioni CSV in evidence finder](#).

Per esportare i 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**). Audit Manager 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.

Per esportare i 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 al [centro download](#) di Audit Manager. 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.

Per trovare il file CSV che cerchi e il file di firma nella console Amazon S3

1. Aprire 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` 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
```

Filtro e opzioni di raggruppamento

Questa pagina descrive le opzioni di filtro e raggruppamento disponibili in evidence finder.

In questa pagina

- [Riferimento al filtro](#)
- [Riferimento di raggruppamento](#)

Riferimento al filtro

Puoi utilizzare i seguenti filtri per trovare prove che soddisfino criteri specifici, come una valutazione, un controllo o Servizio AWS.

Argomenti

- [Filtri obbligatori](#)
- [Filtri aggiuntivi \(facoltativi\)](#)
- [Combinazione di filtri](#)

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.

Nome del filtro	Descrizione	Note
Intervallo di date	Restituisce le prove per un determinato periodo di tempo.	<p>In entrambi i casi, è possibile utilizzare un intervallo relativo per definire un intervallo relativo alla data odierna (ad esempio, Last 30 days).</p> <p>In alternativa, puoi utilizzare un intervallo assoluto per specificare un intervallo di date specifico (ad esempio, June 27th - July 4th).</p>

Nome del filtro	Descrizione	Note
Conformità delle risorse	Restituisce risorse con una valutazione specifica del controllo di conformità.	<p>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. È possibile utilizzare questo filtro per esaminare lo stato di conformità a livello di risorsa.</p> <p>Puoi scegliere una delle seguenti opzioni:</p> <ul style="list-style-type: none">• Non conforme: questo filtro trova risorse con problemi di controllo della conformità. Ciò accade se Security Hub riporta un risultato Non andato a buon fine 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 Andato a buon fine o se AWS Config riporta un risultato conforme.• Inconcludente: questo filtro trova le risorse per le quali un controllo di conformità non è disponibile o applicabile. Ciò accade se una risorsa usa AWS Config Security Hub come tipo di origine dati sottostante, ma tali servizi non sono abilitati. Ciò accade anche se la risorsa usa un tipo di origine dati sottostante che non supporta i controlli di conformità (come prove manuali, chiamate API AWS 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	Espandi entro 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.	<p>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.</p> <p>Esempi di domini di controllo includono la gestione delle identità e degli accessi, la registrazione e il monitoraggio e la gestione della rete.</p>
Data source type (Tipo di origine dati)	Analizza in base al tipo di origine dati.	<p>Usa questi criteri per concentrarti su una fonte di dati specifica.</p> <p>Imposta il valore su <code>Manual</code> per trovare le prove che hai caricato manualmente. Altrimenti, puoi filtrare le prove automatizzate in base alla loro provenienza (ad esempio <code>AWS Config</code>, <code>CloudTrail</code>, <code>Security Hub</code>, o <code>AWS API calls</code>).</p>

Nome del criterio	Descrizione	Quando utilizzare questi criteri
Nome evento	Analizza in base al nome dell'evento.	<p>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.</p> <p>Ad esempio, puoi cercare il nome di una chiamata API, ad esempio l'operazione <code>AttachRolePolicy</code> IAM utilizzato per configurare le autorizzazioni. Oppure, cerca una parola chiave <code>CloudTrail</code>, ad esempio l'evento <code>ConsoleLogin</code> registrato da <code>CloudTrail</code> quando un utente accede al tuo account.</p>
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	Analizza in base alla categoria Servizio AWS.	<p>Utilizza questi criteri per concentrarti su una categoria specifica di Servizio AWS.</p> <p>Gli esempi includono sicurezza, identità e conformità, database e archiviazione.</p>

Combinazione di filtri

Comportamento dei criteri

Quando si specifica più di un criterio, l'Audit Manager 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.

Assessment: MySOC2Assessment

Date range: Last 7 days

Resource compliance [Info](#)
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

Select all

Non-compliant Compliant Inconclusive

Additional filters - optional

Criteria

Control equals Choose a control [Remove](#)

7.2.1 Confirm that access control systems are in place on all system components. [X](#)

and Resource type contains [Remove](#)

AWS::IAM::Policy [X](#)

[Add criteria](#)

Comportamento dei 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 che provengono da AWS CloudTrail, AWS Config, o AWS Security Hub.

and Data source type equals Choose a data source type [Remove](#)

AWS CloudTrail [X](#) AWS Config [X](#) AWS SecurityHub [X](#)

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.
Dominio di controllo	Raggruppa i risultati per dominio 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 nome Servizio AWS.
Categoria di servizio	Raggruppa i risultati per categoria Servizio AWS.

Casi d'uso di esempio

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](#)
- [Caso d'uso 2: Identifica le prove conformi](#)
- [Caso d'uso 3: Esegui una rapida anteprima delle risorse relative alle prove](#)

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](#). 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 in SecOps, IT/DevOps o in un altro ruolo che possiede e ripara le 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 degli stessi criteri (ad esempio, possiedi molteplici 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 Audit Manager.

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 [Anteprima dei riepiloghi delle risorse](#).

Evidence 	Resource ARN	Resource compliance	Date and time
<input type="radio"/> 22615e944-a8b2-4cb0-85e4-d853ea94347b	 arn:aws:iam:us-west1:██████████:policyName	 Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
<input checked="" type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	 arn:aws:cloudtrail:us-west-1:██████████:trail/AWSOrganizationMaster	 Compliant	August 10, 2022, 7:30 (UTC+00:00)
<input type="radio"/> 99615e944-a8b2-4cb0-85e4-d853ea94350d	 arn:aws:cloudtrail:us-west-1:██████████:trail/	 Compliant	August 10, 2022, 7:30 (UTC+00:00)

99615e944-a8b2-4cb0-85e4-d853ea94350d ✕

Resource summary

Resource ARN  arn:aws:iam:us-west1:██████████:policyName	Data source type AWS Config	Assessment PCI DSS V3.2.1 
Resource Type AWS::S3::Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Control domain Identity and access management
Resource compliance  Non-compliant	Account ID ██████████	Control 7.2.1 Confirm that access control systems are in place on all system components.
Date and time August 10, 2022, 7:30 (UTC+00:00)		

Centro di download di Audit Manager

Il centro di download è dove puoi trovare e gestire tutti i tuoi file di Audit Manager scaricabili. Quando generi un report di valutazione o esporti i risultati della ricerca da Evidence Finder, i file vengono visualizzati nel centro di download.

Argomenti

- [Navigazione nel centro di download](#)
- [Scaricamento di un file](#)
- [Eliminazione di un file](#)

Navigazione nel centro di download

Per visitare il centro di download, apri la console di Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>, quindi scegli Centro di download nel riquadro di navigazione a sinistra.

Puoi passare da una scheda all'altra per sfogliare i file per categoria.

Scheda Report di valutazione

Questa scheda mostra tutti i report 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:

- In corso: Audit Manager sta generando il report di valutazione.
- Pronto: il report di valutazione è pronto per essere scaricato.
- Errore: il report di valutazione non è stato generato. In questo caso, Audit Manager visualizza un messaggio che descrive l'errore. Per informazioni su come risolvere questi errori, consulta [Risoluzione dei problemi dei report di valutazione](#).

Scheda Esportazioni

Questa scheda mostra tutti i risultati di 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 CSV, 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:

- In corso: Audit Manager sta preparando il file CSV.
- Pronto: l'esportazione è stata completata e il file è disponibile per il download.
- Errore: l'esportazione non è riuscita. In questo caso, Audit Manager visualizza un messaggio che descrive l'errore. Per informazioni su come risolvere questi errori, consulta [Risoluzione dei problemi di esportazione in formato CSV di Evidence Finder](#).

Note

Tieni presente che la scheda delle esportazioni potrebbe mostrare anche i file CSV delle query che hai eseguito direttamente in AWS CloudTrail Lake. Ciò include le query effettuate nella console CloudTrail o utilizzando l'API CloudTrail. Le esportazioni CloudTrail vengono visualizzate in questa scheda se hai effettuato query nel data store di eventi di Audit Manager e hai scelto di salvare i risultati in 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 AWS Audit Manager 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 dal tuo bucket di destinazione S3, consulta [Download di un oggetto](#) nella Guida per l'utente di Amazon Simple Storage Service (Amazon S3).

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 AWS Audit Manager 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).

Libreria Framework

Puoi accedere e gestire i framework dalla 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 Audit Manager. Puoi utilizzare i framework come punto di partenza per verificare l'utilizzo di Servizio AWS e iniziare ad automatizzare la raccolta delle prove.

La libreria di framework contiene un catalogo di framework standard e personalizzati.

- I framework standard sono framework predefiniti forniti da AWS. Questi framework si basano sulle best practice AWS per diversi standard e normative di conformità. Essi includono 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, puoi personalizzare qualsiasi framework standard per crearne uno nuovo che soddisfi requisiti specifici.

- I framework personalizzati sono framework personalizzati di tua proprietà. Puoi creare un framework personalizzato partendo da zero o personalizzando un framework esistente. Puoi utilizzare framework personalizzati per organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici. Per ulteriori informazioni su come gestire i controlli, consulta [Libreria di controllo](#).

Puoi creare una valutazione da un framework standard o da un framework personalizzato. Per ulteriori informazioni su come creare e gestire le valutazioni, consulta [Valutazioni in AWS Audit Manager](#).

Note

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

Questa sezione descrive come creare e gestire framework personalizzati in Audit Manager.

Argomenti

- [Accesso ai framework disponibili in AWS Audit Manager](#)
- [Visualizzazione dei dettagli di un framework](#)
- [Creazione di un framework personalizzato](#)
- [Modifica di un framework personalizzato](#)
- [Eliminazione di un framework personalizzato](#)
- [Condivisione di un framework personalizzato](#)
- [Framework supportati in AWS Audit Manager](#)

Accesso ai framework disponibili in AWS Audit Manager

Puoi visualizzare tutti i framework disponibili nella pagina della libreria Framework nella console Audit Manager. Da qui, puoi anche [creare una valutazione da un framework](#), [creare un framework personalizzato](#) o [personalizzare un framework esistente](#).

Puoi inoltre visualizzare tutti i framework disponibili utilizzando l'API Audit Manager o AWS Command Line Interface(AWS CLI).

Audit Manager console

Per visualizzare i framework disponibili (console)

1. Apri la console AWS Audit Manager 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.
4. Scegli un nome di framework per visualizzarne i dettagli

AWS CLI

Per visualizzare i framework disponibili (AWS CLI)

Per visualizzare i framework in Audit Manager, utilizza il comando [list-assessment-frameworks](#) e specifica un `--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 (API)

[Utilizza l'operazione ListAssessmentFrameworks 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 i link precedenti per saperne di più nella Guida della AWS Audit Manager Documentazione di riferimento dell'API. Ciò include informazioni su come utilizzare questa operazione `ListAssessmentFrameworkse` questo parametro in uno degli SDK specifici della lingua AWS.

Visualizzazione dei dettagli di un framework

Puoi esaminare i dettagli di un framework utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface(AWS CLI).

Audit Manager console

Per visualizzare i dettagli del framework (console)

1. Apri la console AWS Audit Manager 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.

Quando apri un framework, viene visualizzata una pagina dei dettagli del framework. Le sezioni di questa pagina e il relativo contenuto sono descritti come segue.

Sezione dei dettagli del framework

In questa sezione viene fornita una panoramica di ogni framework. Include le seguenti informazioni:

- Nome del framework: il nome del framework.
- Tipo di conformità: lo standard o il regolamento di conformità supportato dal framework.
- Descrizione: una descrizione del framework, se ne è stata fornita una.
- Tipo di framework: specifica se il framework è un framework standard o personalizzato.
- Set di controlli: il numero di set di controlli associati al framework.
- Controlli: il numero totale di controlli nel framework.
- Origini di controllo: il numero di origini di dati di controllo da cui Audit Manager raccoglie le prove.
- Tag: tag associati al framework.

Se stai visualizzando un framework personalizzato, vengono visualizzati anche i seguenti dettagli:

- Creato da: l'account che ha creato il framework personalizzato.
- Data di creazione: la data di creazione del 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. Include le seguenti informazioni:

- Controlli raggruppati per set di controlli: scegli l'icona della visualizzazione ad albero per visualizzare i controlli che appartengono a ciascun set di controlli.
- Tipo: specifica se il controllo è un controllo standard o personalizzato.
- Origine dati: specifica l'origine dati da cui Audit Manager raccoglie le prove per tale controllo.

Scheda Tag

Questa scheda elenca i tag associati al framework. Include le seguenti informazioni:

- 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 (AWS CLI)

1. Per identificare il framework che desideri esaminare, esegui il comando [list-assessment-frameworks](#) e specifica un `--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 il *testo segnaposto* con Customo 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 comando [get-assessment-framework](#) e specifica il `--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
```

I dettagli del framework vengono restituiti in formato JSON. Per comprendere questi dati, consulta [Output get-assessment-framework](#) nel AWS CLIRiferimento ai comandi

3. Per visualizzare i tag relativi a un framework, usa il comando [list-tags-for-resource](#) e specifica la `--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 Audit Manager, consulta le risorse [Tagging AWS Audit Manager](#).

Audit Manager API

Per visualizzare i dettagli del framework (API)

1. Per identificare il framework che desideri esaminare, esegui il comando [ListAssessmentFrameworks](#) 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, usa l'operazione [GetAssessmentFramework](#). Nella richiesta, specifica il [frameworkId](#) ottenuto dal passaggio 1.

I dettagli del framework vengono restituiti in formato JSON. Per comprendere questi dati, consulta [GetAssessmentFramework Response Elements](#) nella AWS Audit Manager Documentazione di riferimento dell'API.

3. Per visualizzare i tag per il framework, utilizza l'operazione [ListTagsForResource](#). Nella richiesta, specifica il framework [resourceArn](#) ottenuto dal passaggio 1.

Per ulteriori informazioni sull'utilizzo dei tag in Audit Manager, consulta le risorse [Tagging AWS Audit Manager](#).

Per ulteriori informazioni su queste operazioni API, scegli i link precedenti per leggere la AWS Audit Manager Documentazione di riferimento dell'API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS.

Creazione di un framework personalizzato

Puoi accedere e gestire i framework dalla libreria di framework in AWS Audit Manager. Puoi creare framework personalizzati per organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici.

Esistono due modi per creare un framework personalizzato. Puoi personalizzare un framework esistente o puoi crearne uno partendo da zero.

Argomenti

- [Creazione di un nuovo framework personalizzato da zero](#)

- [Personalizzazione di un framework esistente](#)

Creazione di un nuovo framework personalizzato da zero

Puoi utilizzare framework personalizzati in AWS Audit Manager per organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici. Puoi creare un nuovo framework personalizzato partendo da zero nella libreria del framework seguendo questi passaggi.

Argomenti

- [Fase 1: specificare i dettagli del framework](#)
- [Fase 2: specificare i controlli nei set di controlli](#)
- [Fase 3: Revisione e creazione del framework](#)
- [Cosa posso fare dopo?](#)

Fase 1: specificare i dettagli del framework

Inizia specificando i controlli da includere nel framework personalizzato.

Per specificare i dettagli del framework

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel pannello di navigazione a sinistra, scegli Libreria Framework e Crea framework personalizzato.
3. In Dettagli del framework, inserisci un nome, uno standard o un regolamento di conformità (opzionale) e una descrizione per il tuo framework (anch'essa facoltativa). Inserisci una parola chiave relativa allo standard o alla regolamentazione di conformità come PCI_DSS o GDPR in modo da poter utilizzare questa parola chiave per cercare il tuo framework.
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. È possibile utilizzarla come criterio di ricerca quando si cerca questo framework nella libreria Framework. Per ulteriori informazioni sui tag in AWS Audit Manager, consulta [Tagging delle risorse AWS Audit Manager](#).
5. Seleziona Successivo.

Fase 2: specificare i controlli nei set di controlli

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 utilizzi la console AWS Audit Manager per creare un framework personalizzato, puoi aggiungere fino a 10 set di controlli per ogni framework.

Quando utilizzi l'API Audit Manager 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'API [CreateAssessmentFramework](#) fornita da Audit Manager.

Specificare i controlli nei set di controlli

1. Nella sezione Nome del set di controllo, inserisci un nome per il set di controlli.
2. Nella sezione Aggiungi un nuovo controllo al set di controlli, Seleziona il tipo di controllo, utilizza l'elenco a discesa per selezionare uno dei due tipi di controllo: controlli standard o controlli personalizzati. I controlli standard sono forniti da Audit Manager e i controlli personalizzati sono quelli creati dall'utente.
3. In base all'opzione selezionata nel passaggio precedente, viene visualizzato un elenco di controlli standard o controlli personalizzati. Puoi sfogliare l'elenco o effettuare una ricerca inserendo il nome, la conformità o il tag del controllo. Seleziona uno o più controlli e scegli Aggiungi al set di controlli per aggiungerli al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi al set di controlli per confermare l'aggiunta.
5. Nella sezione Esamina i controlli selezionati nel set di controlli, esamina i controlli visualizzati nell'elenco dei controlli selezionati. Per aggiungere altri controlli a un set di controlli, ripeti le fasi da 2 a 4. Puoi rimuovere i controlli indesiderati dal set di controlli selezionando uno o più controlli e scegliendo Rimuovi controllo.
6. Per aggiungere un nuovo set di controlli al framework, scegli Aggiungi set di controlli nella parte inferiore della pagina. Puoi rimuovere i set di controlli indesiderati scegliendo Rimuovi set di controlli.
7. 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](#).

Cosa posso fare dopo?

Dopo aver creato il nuovo framework personalizzato, puoi creare una valutazione a partire dal tuo framework. Per ulteriori informazioni, consulta [Creazione di una valutazione](#).

Puoi inoltre creare un framework personalizzato utilizzando un framework esistente. Per ulteriori informazioni, consulta [Personalizzazione di un framework esistente](#).

Per istruzioni su come modificare il framework personalizzato, consulta [Modifica di un framework personalizzato](#).

Personalizzazione di un framework esistente

Con i framework personalizzati in AWS Audit Manager puoi organizzare i controlli in set di controlli in modo da soddisfare i requisiti specifici. Invece di creare un framework personalizzato partendo da zero, puoi utilizzare un framework esistente come punto di partenza e personalizzarlo. Quando esegui questa operazione, il framework esistente rimane nella libreria del framework e viene creato un nuovo framework personalizzato con le impostazioni personalizzate.

Puoi selezionare qualsiasi framework esistente da personalizzare. Può essere un framework standard o un framework personalizzato.

Nella libreria del framework, dall'elenco a discesa [Crea framework personalizzato](#), scegli [Personalizza framework esistente](#). Attieniti alla seguente procedura per personalizzare il framework.

Argomenti

- [Fase 1: specificare i dettagli del framework](#)
- [Fase 2: specificare i controlli da aggiungere ai set di controlli](#)
- [Fase 3: Revisione e creazione del framework](#)
- [Cosa posso fare dopo?](#)

Fase 1: specificare i dettagli del framework

Tutti i dettagli del framework, tranne i tag, vengono trasferiti dal framework originale. Rivedi e modifica questi dettagli in base alle esigenze.

Per specificare i dettagli del framework

1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione a sinistra, scegli Libreria Framework.
3. Scegli il framework che desideri personalizzare e dall'elenco a discesa Crea framework personalizzato, scegli Personalizza framework esistente.
4. Nella finestra pop-up che appare, inserisci un nome per il nuovo framework personalizzato e scegli Personalizza.
5. Nella sezione 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 di tag è obbligatoria e può essere utilizzata come criterio di ricerca quando cerchi questo framework nella Libreria framework. Per ulteriori informazioni sui tag in AWS Audit Manager, consulta [Tagging delle risorse AWS Audit Manager](#).
7. Seleziona Successivo.

Fase 2: specificare i controlli da aggiungere ai set di controlli

I set di controllo vengono trasferiti dal framework originale. Personalizza la configurazione attuale aggiungendo altri controlli o rimuovendo i controlli esistenti in base alle esigenze.

Note

Quando utilizzi la console AWS Audit Manager per personalizzare un framework, puoi aggiungere fino a 10 set di controlli per ogni framework.

Quando utilizzi l'API Audit Manager 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'API [CreateAssessmentFramework](#) fornita da Audit Manager.

Per specificare i controlli nei set di controlli

1. Nella sezione Nome del set di controlli, personalizza il nome del set di controlli in base alle esigenze.
2. Nella sezione Aggiungi un nuovo controllo al set di 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. Puoi sfogliare l'elenco o effettuare una ricerca inserendo il nome, la conformità o il tag del controllo per individuare i controlli che desideri aggiungere. Seleziona uno o più controlli e scegli Aggiungi al set di controlli per aggiungerli al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi al set di controlli per confermare l'aggiunta.
5. Nella sezione Esamina i controlli selezionati nel set di controlli, esamina i controlli visualizzati nell'elenco dei controlli selezionati. Per aggiungere altri controlli a un set di controlli, ripeti le fasi da 2 a 4. Puoi rimuovere i controlli indesiderati dal set di controlli selezionando uno o più controlli e scegliendo Rimuovi controllo.
6. Per aggiungere un nuovo set di controlli al framework, scegli Aggiungi set di controlli nella parte inferiore della pagina. Puoi rimuovere i set di controlli indesiderati scegliendo Rimuovi set di controlli.
7. 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.

Cosa posso fare dopo?

Dopo aver creato il nuovo framework personalizzato, puoi creare una valutazione a partire dal tuo framework. Per ulteriori informazioni, consulta [Creazione di una valutazione](#).

Per istruzioni su come modificare il framework personalizzato, consulta [Modifica di un framework personalizzato](#).

Modifica di un framework personalizzato

Puoi utilizzare framework personalizzati in AWS Audit Manager per organizzare i controlli in set di controlli in modo da soddisfare le tue esigenze specifiche. Puoi utilizzare la libreria di framework per trovare e modificare un framework personalizzato seguendo questi passaggi.

Argomenti

- [Fase 1: modificare dettagli del framework](#)
- [Fase 2: modificare i controlli nei set di controlli](#)
- [Fase 3. Revisione e aggiornamento del framework](#)

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 AWS Audit Manager 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, puoi aprire un framework personalizzato e scegliere Azioni, Modifica in alto a destra nella pagina di riepilogo della valutazione.
4. Nella sezione Dettagli del framework, esamina il nome, il tipo di conformità e la descrizione del framework e apporta le modifiche necessarie.
5. Seleziona Successivo.

i 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: modificare i controlli nei set di controlli

Successivamente, rivedi e modifica i controlli e i set di controlli nel framework.

i Note

Quando utilizzi la console AWS Audit Manager per modificare un framework personalizzato, puoi aggiungere fino a 10 set di controlli per ogni framework.

Quando utilizzi l'API Audit Manager 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'API [UpdateAssessmentFramework](#) fornita da Audit Manager.

Per modificare i controlli

1. Nella sezione Nome del set di controlli, rivedi e modifica il nome del set di controlli secondo le necessità.
2. Nella sezione Aggiungi un nuovo controllo al set di controlli, puoi aggiungere un controllo. Utilizza 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 a tabella di controlli standard o controlli personalizzati. Puoi sfogliare l'elenco dei set di controlli. Oppure, puoi effettuare una ricerca inserendo il nome, l'origine dati, o i tag del controllo per individuare i controlli che desideri aggiungere. Seleziona uno o più controlli e scegli Aggiungi al set di controlli per aggiungerli al set di controlli.
4. Nella finestra pop-up che appare, scegli Aggiungi al set di controlli per confermare l'aggiunta.
5. Nella sezione Esamina i controlli selezionati nel set di controlli, esamina e modifica i controlli attualmente visualizzati nell'elenco dei controlli selezionati. Per aggiungere altri controlli a un set di controlli, ripeti le fasi da 2 a 4. Rimuovi i controlli indesiderati dal set di controlli selezionando uno o più controlli e scegliendo Rimuovi controllo.

6. Per aggiungere un nuovo set di controlli al framework, scegli **Aggiungi set di controlli** nella parte inferiore della pagina. Rimuovi i set di controlli indesiderati scegliendo **Rimuovi set di controlli**.
7. Dopo aver aggiunto i set di controlli e i controlli, seleziona **Successivo**.

Fase 3. Revisione e aggiornamento del framework

Rivedi le informazioni del tuo framework. Per modificare le informazioni relative a una fase, scegli **Modifica**.

Al termine, scegli **Salva le modifiche**.

Eliminazione di un framework personalizzato

Puoi utilizzare la libreria di framework per trovare ed eliminare un framework personalizzato indesiderato. Puoi inoltre eliminare i framework personalizzati utilizzando 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

Come aggiornare un framework personalizzato (console)

1. Apri la console AWS Audit Manager 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

Come aggiornare un framework personalizzato (AWS CLI)

1. Innanzitutto, identifica il framework personalizzato da eliminare. Per farlo, esegui il comando [list-assessment-frameworks](#) e specifica il `--framework-type` come 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 comando [delete-assessment-framework](#) e specifica il `--framework-id` del 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 aggiornare un framework personalizzato (API)

1. Utilizza l'operazione [ListAssessmentFrameworks](#) e specifica un [frameworkType](#) come Custom. Trova la risposta, trova il framework personalizzato che desideri eliminare e prendi nota dell'ID del framework.
2. Utilizza l'operazione [DeleteAssessmentFramework](#) per eliminare il framework. Nella richiesta, utilizza il parametro [frameworkId](#) per specificare il framework che desideri eliminare.

Per ulteriori informazioni su queste operazioni API, scegli i link precedenti per leggere la AWS Audit Manager Documentazione di riferimento dell'API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS.

Condivisione di un framework personalizzato

Puoi utilizzare la funzionalità di condivisione del framework di AWS Audit Manager per replicare rapidamente i framework personalizzati che crei. Puoi condividere i tuoi framework personalizzati

con altri Account AWS replicare i tuoi framework in un altro Regione AWS con il tuo account. 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.

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, Audit Manager replica il framework personalizzato condiviso nella sua libreria di framework. Oltre a replicare il framework personalizzato, Audit Manager 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. Audit Manager non replica framework o controlli standard. Per impostazione predefinita, sono disponibili in tutti gli Account AWS e le regioni in cui è abilitato Audit Manager.

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 [AWS Audit Manager pagina dei prezzi](#).

Important

Se il framework standard è indicato come non idoneo alla condivisione da AWS non puoi condividere un framework personalizzato derivato da un framework standard, a meno che tu non abbia ottenuto l'autorizzazione a farlo 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](#).

Le seguenti sezioni della presente guida descrivono gli elementi importanti da sapere sulla condivisione del framework. Forniscono inoltre istruzioni su come condividere i framework personalizzati e rispondere alle richieste di condivisione.

Argomenti

- [Concetti e terminologia di condivisione dei framework](#)
- [Invio di una richiesta di condivisione per un framework personalizzato](#)
- [Risposta alle richieste di condivisione](#)
- [Eliminazione di richieste di condivisione](#)

i Tip

Se non conosci i framework personalizzati di Audit Manager e non sai come crearli, puoi saperne di più nella pagina [Creazione di un framework personalizzato](#) della presente guida.

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.

Mittente

Si tratta del creatore di una richiesta di condivisione e l'Account AWS in cui si trova il framework personalizzato. I mittenti possono condividere framework personalizzati con qualsiasi Account AWS. Oppure, possono replicare un framework personalizzato su qualsiasi framework supportato da Regione AWS dal proprio account.

Destinatario

Si tratta del consumatore del framework condiviso. I destinatari possono accettare o rifiutare una richiesta di condivisione da parte di un mittente.

i Note

Un destinatario può essere un account da amministratore delegato. Tuttavia, non è possibile condividere framework personalizzati con un account di gestione AWS Organizations.






Idoneità al framework

È possibile condividere solo framework personalizzati. Per impostazione predefinita, i framework standard sono già presenti in tutti gli Account AWS e Regioni AWS dove è abilitato 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. Se il framework standard è indicato come non idoneo alla condivisione da AWS non puoi condividere un framework personalizzato derivato da un framework standard, a meno che tu non abbia ottenuto l'autorizzazione a farlo 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 dell'Australian Cyber Security Center (ACSC)	 Sì
AWS Audit Manager Framework di esempio	 Sì
AWS Control Tower Guardrail	 Sì
AWS framework generativo per le best practice di intelligenza artificiale v1	 Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione
AWS License Manager	 Sì
AWS Foundational Security Best Practices	 Sì
AWS Best practice operative	 Sì
Canone di architettura AWS	 Sì
Centro canadese per la sicurezza informatica - Medio	 No
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1	 No
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1 e 2	 No
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0, Livello 1	 No

Nome del framework standard	Versioni personalizzate idonee alla condivisione
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0, Livello 1 e 2	 No
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0, Livello 1	 No
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0, Livello 1 e 2	 No
Controlli CIS v7.1 IG1	 Sì
Controlli CIS v8 IG1	 No
FedRAMP Moderate Baseline	 Sì
GDPR	 Sì
Gramm-Leach-Bliley Act (GLBA)	 Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione
GxP 21 CFR Parte 11	 Sì
GxP UE Allegato 11	 Sì
Norma di sicurezza HIPAA 2003	 Sì
Norma di sicurezza Omnibus finale HIPAA 2013	 Sì
ISO/IEC 27001:2013 Allegato A	 No
NIST 800-53 (Rev. 5) Low-Moderate-High	 Sì
Framework NIST per la sicurezza informatica versione 1.1	 Sì
NIST SP 800-171 Rev. 2	 Sì

Nome del framework standard	Versioni personalizzate idonee alla condivisione
PCI DSS v3.2.1	 No
PCI DSS v4.0	 No
SOC 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.

- **Attiva:** indica una richiesta di condivisione che è stata inviata correttamente al destinatario ed è in attesa della sua risposta.
- **In scadenza:** indica una richiesta di condivisione che scade entro i prossimi 30 giorni.
- **Condivisa:** indica una richiesta di condivisione accettata dal destinatario.
- **Inattiva:** indica una richiesta di condivisione che è stata revocata, rifiutata o scaduta prima di eventuali azioni da parte del destinatario.
- **In fase di replica:** indica una richiesta di condivisione accettata che viene replicata nella libreria di framework del destinatario.

- **Non riuscita:** indica una richiesta di condivisione che non è stata inviata correttamente al destinatario.

Notifiche di richiesta di condivisione

Audit Manager 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, Audit Manager crea una copia indipendente del framework personalizzato nella libreria del framework del destinatario.

Oltre a replicare il framework personalizzato del mittente, Audit Manager replica anche tutti i set di controlli e i controlli personalizzati contenuti in tale framework. Tuttavia, Audit Manager 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, Audit Manager 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, Audit Manager 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 crei una richiesta di condivisione, Audit Manager archivia un'istantanea del framework personalizzato nella Regione AWS Stati Uniti orientali (Virginia settentrionale). Audit Manager archivia anche un backup della stessa istantanea nella Regione AWS Stati Uniti occidentali (Oregon).

Audit Manager 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 suo Account AWS specificata nella Regione AWS specificata nella richiesta di condivisione.

Controllo delle versioni del framework condiviso

Quando condividi un framework personalizzato, Audit Manager crea una copia indipendente di tale framework nell'Account AWS e nella regione 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 con un altro Regione AWS tramite il tuo account e poi elimini quel framework personalizzato nella prima 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.

Invio di una richiesta di condivisione per un framework personalizzato

Questo tutorial descrive come condividere i framework personalizzati tra Account AWS e Regioni AWS.

Quando condividi un framework personalizzato, Audit Manager 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, Audit Manager 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 ID Account AWS come ID dell'account del destinatario.

Questa esercitazione contiene i seguenti passaggi:

1. [Seleziona un framework da condividere](#): sfoglia la libreria del framework per trovare il framework personalizzato che desideri condividere.
2. [Invia una richiesta di condivisione](#): specifica un destinatario e inviagli una richiesta di condivisione per il framework personalizzato.
3. [Visualizza le richieste inviate](#): visualizza la cronologia delle richieste di condivisione e controlla lo stato delle richieste inviate.
4. [\(Facoltativo\) Revoca la richiesta di condivisione](#): revoca la richiesta di condivisione prima della scadenza.

Prerequisiti

Prima di iniziare questo tutorial, assicurati che siano soddisfatte le seguenti condizioni:

- Conosci il [framework che condivide concetti e terminologia](#) Audit Manager.
- 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 ha già abilitato AWS Audit Manager nella Regione AWS in cui desideri condividere il framework personalizzato.
- Il destinatario non è un account di gestione AWS Organizations.

Tip

Prima di iniziare, prendi nota dell'ID Account AWS 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'altra Regione AWS nel tuo account. Queste informazioni serviranno per la fase 2 del tutorial.

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](#).

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 Audit Manager.

Per visualizzare i framework personalizzati disponibili

1. Apri la console AWS Audit Manager 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 Audit Manager 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 regole AWS Config personalizzate come origine dati, ti consigliamo di contattare il destinatario per informarlo. Il destinatario può quindi creare e abilitare le stesse regole AWS Config nella propria istanza di AWS Config. Per ulteriori informazioni, consulta [Il mio framework condiviso ha controlli che utilizzano AWS Config regole personalizzate come fonte di dati. Il destinatario può raccogliere prove per questi controlli?](#)
3. Inserisci **agreee** 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 Regione AWS specificata. Dopo aver accettato la richiesta di condivisione, il destinatario può quindi replicare il framework tra le regioni, se necessario.
- Quando si condividono framework personalizzati tra 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, Audit Manager 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.
 - Attive: questo filtro mostra le richieste di condivisione in attesa di risposta dal destinatario.
 - Condiviso: questo filtro mostra le richieste di condivisione accettate dal destinatario. Il framework personalizzato condiviso ora esiste nella libreria di framework del destinatario.

- **Inattive:** il filtro visualizza le richieste di condivisione revocate, rifiutate o scadute prima di eventuali azioni da parte del destinatario. Scegli la parola Inattive per visualizzare ulteriori dettagli.
- **In scadenza:** questo filtro mostra le richieste di condivisione che scadono nei prossimi 30 giorni.
- **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. Ti consigliamo di ricontrollare in un secondo momento per confermare che la richiesta di condivisione è stata inviata correttamente.

Per informazioni su come procedere in caso di errore, consulta [Risoluzione dei problemi relativi alle richieste di condivisione](#).

Fase 4 (facoltativo): revoca della richiesta di condivisione

Se devi annullare una richiesta di condivisione attiva prima della scadenza, puoi revocarla in qualsiasi momento. Questo passaggio è facoltativo. 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 Regioni AWS, possono essere necessari fino a 10 minuti per elaborare le azioni di richiesta di condivisione. 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.

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 attivo, condiviso 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 AWSdestinatario. 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. 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 Audit Manager prepara la richiesta di condivisione.
2. Esamina l'avviso visualizzato nella finestra di dialogo, inserisci **agree**, quindi scegli Accetto per procedere.
 3. 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.
 4. Scegli Condividi per inviare nuovamente e aggiornare la richiesta di condivisione.

Risoluzione dei problemi di richieste di condivisione

Per trovare soluzioni ai problemi che potresti riscontrare quando condividi un framework personalizzato, consulta [Risoluzione dei problemi di condivisione del framework](#) nella sezione Risoluzione dei problemi di questa guida.

Risposta alle richieste di condivisione

Questo tutorial descrive le azioni da eseguire quando ricevi una richiesta di condivisione per un framework personalizzato. Audit Manager ti avvisa quando ricevi una richiesta di condivisione. Riceverai una notifica anche quando una richiesta di condivisione sta per scadere nei prossimi 30 giorni.

Questo tutorial contiene i seguenti passaggi:

1. [Controlla le notifiche delle tue richieste di condivisione](#): esamina un elenco di richieste di condivisione attive e in scadenza a breve.

2. [Agisci sulla richiesta di condivisione](#): accetta o rifiuta la richiesta di condivisione per il framework personalizzato.
3. [Visualizza le richieste di condivisione che hai ricevuto da altri](#): visualizza la cronologia delle richieste di condivisione.

Prerequisiti

Prima di iniziare, ti consigliamo di approfondire la [condivisione dei concetti e della terminologia del framework](#) Audit Manager.

Fase 1: verifica delle notifiche di richiesta ricevute

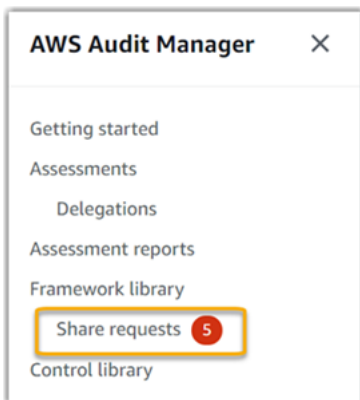
Inizia controllando le notifiche di richiesta di condivisione. La scheda Richieste ricevute mostra un elenco delle richieste di condivisione che hai ricevuto da altri Account AWS. Le richieste in attesa di risposta vengono visualizzate con un punto blu. Puoi anche filtrare questa visualizzazione per visualizzare solo le richieste che scadono entro i prossimi 30 giorni.

Per visualizzare le richieste ricevute

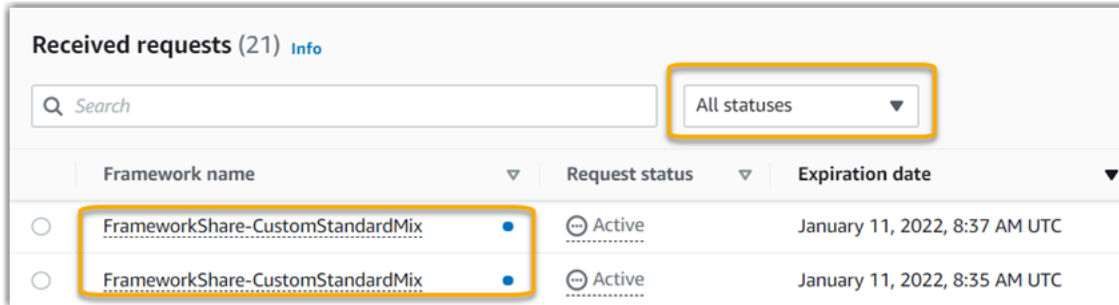
1. Apri la console AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Se hai una notifica di richiesta di condivisione, Audit Manager visualizza un punto rosso accanto all'icona del menu di navigazione.



3. Espandi il riquadro di navigazione e guarda accanto a Condividi richieste. Un badge di notifica indica il numero di richieste di condivisione che richiedono la tua attenzione.



- Scegli Condividi richieste. Per impostazione predefinita, questa pagina si apre sulla scheda Richieste ricevute.
- Identifica le richieste di condivisione che richiedono la tua azione cercando gli elementi con un punto blu.



- (Facoltativo) Per visualizzare solo le richieste che scadono 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.

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.

Accettare un framework condiviso

Quando accetti una richiesta di condivisione, Audit Manager replica un'istantanea del framework originale nella scheda framework personalizzati della libreria del framework. Audit Manager replica e crittografa il nuovo framework personalizzato utilizzando la chiave KMS specificata nelle [impostazioni di Audit Manager](#).

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, Audit Manager 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.

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 AWS Audit Manager 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.
 - Attive: 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.
 - Condivise: questo filtro mostra le richieste di condivisione che hai accettato. Il framework condiviso è ora disponibile nella tua libreria di framework.
 - Inattive: questo filtro mostra le richieste di condivisione rifiutate o scadute.
 - Non riuscite: questo filtro mostra le richieste di condivisione che non sono state inviate correttamente. Scegli la parola Non riuscite per visualizzare ulteriori dettagli.

Cosa posso fare dopo?

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](#). Per istruzioni su come modificare il nuovo framework personalizzato, consulta [Modifica di un framework personalizzato](#).

Eliminazione di richieste di condivisione

Puoi eliminare le richieste di condivisione che non sono più desiderate o necessarie.

Note

Non è possibile eliminare le richieste di condivisione con stato attive o in fase di replica. Quando elimini una richiesta di condivisione, viene eliminata solo la richiesta. Il framework condiviso rimane nella libreria del framework.

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.

Framework supportati in AWS Audit Manager

AWS Audit Manager fornisce i seguenti framework standard. Questi framework predefiniti si basano sulle best practice AWS per vari standard e normative di conformità. È possibile utilizzare questi framework per facilitare la preparazione degli audit.

Argomenti

- [Essential Eight dell'Australian Cyber Security Center \(ACSC\)](#)
- [Manuale sulla sicurezza delle informazioni dell'Australian Cyber Security Center \(ACSC\)](#)
- [Framework di esempio AWS Audit Manager](#)
- [Guardrail AWS Control Tower](#)

- [Framework di best practice di IA generativa AWSv1](#)
- [AWS License Manager](#)
- [AWS Foundational Security Best Practices](#)
- [Best practice operative AWS](#)
- [AWS Well-Architected](#)
- [Canadian Centre for Cyber Security Medium Cloud Control Profile](#)
- [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0](#)
- [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0](#)
- [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0](#)
- [Gruppo di implementazione 1 di CIS Controls v7.1](#)
- [Gruppo di implementazione 1 di CIS Controls v8](#)
- [FedRAMP Moderate Baseline](#)
- [Regolamento generale sulla protezione dei dati \(GDPR\)](#)
- [Gramm-Leach-Bliley Act](#)
- [GxP 21 CFR parte 11](#)
- [GxP UE Allegato 11](#)
- [Norma di sicurezza Health Insurance Portability and Accountability Act \(HIPAA\) 2003](#)
- [Norma di sicurezza Omnibus finale Health Insurance Portability and Accountability Act \(HIPAA\) 2013](#)
- [ISO/IEC 27001:2013 Allegato A](#)
- [NIST 800-53 \(Rev. 5\) Low-Moderate-High](#)
- [Framework NIST per la sicurezza informatica versione 1.1](#)
- [NIST SP 800-171 \(Rev. 2\)](#)
- [PCI DSS V3.2.1](#)
- [PCI DSS V4.0](#)
- [SOC 2](#)

Essential Eight dell'Australian Cyber Security Center (ACSC)

Per aiutarti nella preparazione degli audit, AWS Audit Manager fornisce un framework standard predefinito che struttura e automatizza le valutazioni per il framework Essential Eight.

Argomenti

- [Cos'è l'Essential Eight dell'Australian Cyber Security Center \(ACSC\)?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse Essential Eight](#)

Cos'è l'Essential Eight dell'Australian Cyber Security Center (ACSC)?

L'Australian Cyber Security Centre (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).

L'[Essential Eight](#) di [ACSC](#) è concesso in licenza con una [licenza internazionale Creative Commons Attribution 4.0](#) e le informazioni sul copyright sono disponibili all'indirizzo [ACSC | Copyright](#). © Commonwealth of Australia 2022.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework standard Essential Eight AWS Audit Manager che ti aiuterà 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
Essential Eight	7	1	8	<ul style="list-style-type: none"> • AWS Config • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_EssentialEight.zip](#).

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

Puoi trovare il framework Essential Eight nella scheda Frameworks standard della [Libreria Framework](#) di Audit Manager.

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. La selezione viene effettuata in base ai requisiti del framework Essential Eight. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#). Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse Essential Eight

- [ACSC Essential Eight](#)

Manuale sulla sicurezza delle informazioni dell'Australian Cyber Security Center (ACSC)

Per aiutarti nella preparazione degli audit, AWS Audit Manager fornisce un framework standard predefinito che struttura e automatizza le valutazioni per il framework del Manuale sulla sicurezza delle informazioni ACSC.

Argomenti

- [Cos'è il Manuale sulla sicurezza delle informazioni dell'Australian Cyber Security Center \(ACSC\)?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Ulteriori risorse sul Manuale sulla sicurezza delle informazioni ACSC](#)

Cos'è il Manuale sulla sicurezza delle informazioni dell'Australian Cyber Security Center (ACSC)?

L'Australian Cyber Security Centre (ACSC) è l'agenzia principale del governo australiano per la sicurezza informatica. L'ACSC produce il Manuale sulla sicurezza delle informazioni (ISM), che funziona come un insieme di principi sulla 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.

[Il framework ISM è fornito dall'Australian Cyber Security Centre con una licenza internazionale Creative Commons Attribution 4.0 e le informazioni sul copyright sono disponibili all'indirizzo ACSC | Copyright.](#) © Commonwealth of Australia 2022.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework standard del Manuale sulla sicurezza delle informazioni dell'ACSC in AWS Audit Manager 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 del Manuale sulla sicurezza delle informazioni ACSC. 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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. Tale operazione avviene sulla base dei controlli definiti nel framework del Manuale sulla sicurezza delle informazioni dell'ACSC. 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	Servizi AWS nell'ambito di applicazione
Manuale sulla sicurezza delle informazioni ACSC	45	396	22	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip](#)

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

È possibile trovare il framework del Manuale sulla sicurezza delle informazioni ACSC nella scheda Framework standard del [Libreria Framework](#) di Audit Manager.

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework del Manuale sulla sicurezza delle informazioni dell'ACSC. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#). Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Ulteriori risorse sul Manuale sulla sicurezza delle informazioni ACSC

- [Manuale sulla sicurezza delle informazioni ACSC](#)

Framework di esempio AWS Audit Manager

AWS Audit Manager fornisce un framework di esempio per consentirti di iniziare a preparare l'audit.

Argomenti

- [Cos'è il framework di esempio AWS Audit Manager?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)

Cos'è il framework di esempio AWS Audit Manager?

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 Audit Manager, 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 chiamate API AWS Config AWS.

Utilizzo di questo framework a supporto della preparazione dell'audit

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

Utilizzando il AWS Audit Manager framework di esempio come punto di partenza, puoi creare una valutazione Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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 di esempio AWS Audit Manager sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Framework di esempio AWS Audit Manager	4	1	3	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del Framework di esempio AWS Audit Manager. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Guardrail AWS Control Tower

AWS Audit Manager fornisce un framework guardrail AWS Control Tower per facilitare la preparazione degli audit.

Argomenti

- [Cos'è AWS Control Tower?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse AWS Control Tower](#)

Cos'è AWS Control Tower?

AWS Control Tower è un servizio di gestione e governance che puoi utilizzare per navigare nel processo di configurazione e nei requisiti di governance coinvolti nella creazione di un ambiente AWS multi-account.

Con AWS Control Tower, puoi fornire nuovi Account AWS conformi alle policy aziendali o organizzative in pochi clic. AWS Control Tower crea per conto tuo un livello di orchestrazione che combina e integra le funzionalità di diversi altri [AWS servizi](#). Tra questi servizi figurano AWS Organizations, AWS IAM Identity Center Servizio AWS Catalog. In questo modo puoi semplificare il processo di configurazione e gestione di un ambiente AWS multi-account sicuro e conforme.

Il framework Guardrails AWS Control Tower contiene tutti i Regole di AWS Config basati sui guardrail di AWS Control Tower.

Utilizzo di questo framework a supporto della preparazione dell'audit

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 secondo il Regole di AWS Config in base ai guardrail 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 audit AWS Control Tower. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework Guardrails AWS Control Tower. 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 Guardrails AWS Control Tower sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Guardrail AWS Control Tower	14	0	5	AWS Config

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip](#).

I controlli di questo framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi ai Guardrails AWS Control Tower. Inoltre, non possono garantire il superamento dell'audit.

Puoi trovare il framework Guardrails AWS Control Tower nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare o aggiornare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. La selezione viene effettuata in base ai requisiti dei Guardrails AWS Control Tower. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse AWS Control Tower

- [AWS Control Tower pagina dei servizi](#)
- [AWS Control Tower guida per l'utente](#)

Framework di best practice di IA generativa AWSv1

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

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

Argomenti

- [Cosa sono le best practice di IA generativa AWS per Amazon Bedrock?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Verifica manuale delle istruzioni in Amazon Bedrock](#)
- [Altre risorse](#)

Cosa sono le best practice di IA generativa AWS 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 per creare il AWSframework delle best practice per l'IA generativa v1. Questo framework ti fornisce uno strumento specifico per monitorare e migliorare la governance dei tuoi progetti di IA generativa su Amazon Bedrock. 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 IA, professionisti della conformità, specialisti di garanzia della sicurezza AWS e con il contributo di Deloitte. Ogni controllo automatizzato è mappato a un'origine dati AWS dalla quale 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:** impedisce 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 di best practice dell'IA generativa AWS 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)
- Implementazione della crittografia end-to-end per i dati di input e output dei modelli di IA secondo gli standard minimi del settore (Sicurezza)

Utilizzo di questo framework a supporto della preparazione dell'audit

Note

- Se sei un cliente Amazon Bedrock, puoi utilizzare questo framework direttamente in Audit Manager. Assicurati di utilizzare il framework ed eseguire valutazioni negli Account AWS nelle regioni in cui esegui i modelli e le applicazioni di IA generativa.
- Se desideri crittografare i log di CloudWatch per Amazon Bedrock con la tua chiave KMS, assicurati che Audit Manager abbia accesso a quella chiave. A tale scopo, puoi salvare la chiave gestita dal cliente nelle impostazioni [Crittografia dei dati](#) di Audit Manager.
- Questo framework utilizza l'operazione [ListCustomModels](#) Amazon Bedrock per generare prove sull'utilizzo del modello personalizzato. Questa operazione API è attualmente supportata solo nelle Regioni AWS Stati Uniti orientali (Virginia settentrionale) e Stati Uniti occidentali (Oregon). 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'IA generativa su Amazon Bedrock. 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 Audit Manager 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 risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework delle best practice per l'IA generativa AWS. 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	Servizi AWS nell'ambito di applicazione
Framework delle best practice di IA generativa AWSv1	8	34 completamente automatizzato 18 parzialmente automatizzato	58	<ul style="list-style-type: none"> • Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Tip

Per ulteriori informazioni sui controlli automatici e manuali, consulta [Concetti e terminologia di Audit Manager](#) per un esempio di quando è consigliabile aggiungere prove manuali a un controllo parzialmente automatizzato.

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati di controllo in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip](#).

I controlli di questo framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi alle best practice di IA generativa. Inoltre, non possono garantire il superamento di un audit sull'utilizzo dell'IA generativa. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#). Per istruzioni su come creare una copia modificabile di questo framework per supportare requisiti specifici, vedere [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

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'operazione [InvokeModel](#) fornita da Amazon Bedrock. Puoi quindi raccogliere le risposte del modello a queste richieste e [caricare questi dati come prove manuali](#) nella valutazione dell'Audit Manager.

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 supportata 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

Puoi 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 con l'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 *invoke-model-output.txt*:

```
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 utilizzare i canary CloudWatch Synthetics per monitorare le risposte del tuo modello. Con questa soluzione, puoi verificare il risultato `InvokeModel` di un elenco di prompt predefiniti e quindi utilizzare CloudWatch per monitorare il comportamento del modello 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, *****"

```

Altre risorse

- [Amazon Bedrock](#)
- [Guida per l'utente di Amazon Bedrock](#)
- [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 framework AWS License Manager per facilitare la preparazione degli audit.

Argomenti

- [Cos'è AWS License Manager?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse AWS License Manager](#)

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 e ambienti on-premise. 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 framework AWS License Manager 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 a supporto della preparazione dell'audit

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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework AWS License Manager. 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 License Manager sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
AWS License Manager	27	0	6	AWS License Manager

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework AWS License Manager. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse AWS License Manager

Collegamenti License Manager

- [AWS License Manager pagina dei servizi](#)
- [AWS License Manager guida per l'utente](#)

API License Manager

Per questo framework, Audit Manager 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'attività `GetLicenseManagerSummary` richiama l'API [ListLicenseConfigurations](#), che fornisce dettagli sulle configurazioni delle licenze nell'account. Successivamente, aggiunge dati contestuali aggiuntivi per ogni configurazione di licenza chiamando [ListUsageForLicenseConfiguration](#) e [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 and 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 Foundational Security Best Practices

AWS Audit Manager fornisce un framework standard predefinito che supporta AWS Foundational Security Best Practices.

Argomenti

- [Cos'è lo standard AWSFoundational Security Best Practices?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Ulteriori risorse su AWSFoundational Security Best Practices](#)

Cos'è lo standard AWSFoundational Security Best Practices?

Lo standard AWSFoundational Security Best Practices è un insieme di controlli che rilevano quando gli account e le risorse distribuiti si discostano dalle best practice per la sicurezza.

Lo standard consente di valutare continuamente tutti i tuoi Account AWS e carichi di lavoro per 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 a supporto della preparazione dell'audit

Puoi utilizzare il framework AWSFoundational 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 AWSFoundational 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le risorse nei tuoi Account AWS e servizi. La valutazione avviene sulla base dei controlli definiti nel framework AWSFoundational 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 AWSFoundational 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	Servizi AWS nell'ambito di applicazione
AWS Foundational Security Best Practices	154	0	29	AWS Security Hub

I controlli di questo framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi a AWS Foundational Security Best Practices. Inoltre, non possono garantire il superamento di un audit AWS Foundational Security Best Practices.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti AWS Foundational Security Best Practices. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Ulteriori risorse su AWS Foundational Security Best Practices

- [Standard AWS Foundational Security Best Practices](#) nella AWS Security Hub Guida per l'utente
- [Categorie di controllo](#) nella AWS Security Hub Guida per l'utente

Best practice operative AWS

AWS Audit Manager fornisce un framework predefinito Best practices operative (OBP) AWS per facilitare la 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?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse OBP AWS](#)

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 a supporto della preparazione dell'audit

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 best practice operative AWS. 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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le risorse nei tuoi Account AWS e servizi. La valutazione avviene sulla base dei controlli definiti nel framework delle best practice operative AWS. 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 Best practice operative AWS sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Best practice operative AWS	52	0	20	AWS Security Hub

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi alle best practice operative AWS. Inoltre, non possono garantire il superamento di un audit sulle best practice operative AWS.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti delle best practice operative AWS. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse OBP AWS

- [Standard AWS Foundational Security Best Practices](#) nella Guida per l'utente AWS Security Hub
- [Categorie di controllo](#) nella AWS Security Hub Guida per l'utente

AWS Well-Architected

AWS Audit Manager fornisce un framework predefinito che struttura e automatizza le valutazioni per il framework AWS Well-Architected, sulla base delle best practice AWS.

Argomenti

- [Che cos'è AWS Well-Architected?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse AWS Well-Architected](#)

Che cos'è AWS Well-Architected?

[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 a supporto della preparazione dell'audit

Puoi utilizzare il framework AWS Well-Architected 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. Lo fa in base ai controlli definiti nel framework AWS Well-Architected. 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 AWSWell-Architected sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Framework AWSWell-Architected	16	0	2	AWS Config

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip](#).

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi. Inoltre, non possono garantire il superamento di un audit associato al framework AWSWell-Architected.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework AWSWell-Architected. Se è necessario modificare l'elenco dei servizi in

ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse AWSWell-Architected

- [AWS Well-Architected](#)
- [Documentazione del framework AWSWell-Architected](#)

Canadian Centre for Cyber Security Medium Cloud Control Profile

AWS Audit Manager fornisce un framework standard predefinito che struttura e automatizza le valutazioni per il Centro canadese per la sicurezza informatica.

Argomenti

- [Cos'è il Centro canadese per la sicurezza informatica?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)

Cos'è il Centro canadese per la sicurezza informatica?

Il Centro canadese per la sicurezza informatica (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 a supporto della preparazione dell'audit

Puoi utilizzare il framework AWS Audit Manager per il Medium Cloud Control Profile 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 CCCS Medium Cloud Control Profile. Nella valutazione, puoi specificare gli Account AWS e i servizi che desideri includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework CCCS Medium Cloud Control Profile. 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	Servizi AWS nell'ambito di applicazione
Centro canadese per la sicurezza informatica - Medio	206	396	165	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

 Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file

[AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip](#).

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework del Centro canadese per la sicurezza informatica - Medio. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0

AWS Audit Manager fornisce due framework predefiniti che supportano il CIS AWSFoundations Benchmark v1.2.0:

- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1
- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1 e 2

Note

- Per informazioni sui framework Audit Manager che supportano la versione 1.3.0, consulta [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0](#).
- Per informazioni sui framework Audit Manager che supportano la versione 1.4.0, consulta [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0](#).

Argomenti

- [Cos'è il CIS?](#)
- [Utilizzo di questi framework a supporto della preparazione dell'audit](#)
- [Altre risorse CIS](#)

Cos'è il CIS?

[Il Center for Internet Security \(CIS\) è un'organizzazione no profit che ha sviluppato il CIS AWSFoundations Benchmark](#). 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, in quanto forniscono procedure di implementazione e valutazione chiare e dettagliate.

Per ulteriori informazioni, consulta i [post del blog CIS AWSFoundations Benchmark](#) sul Blog sulla sicurezza 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 Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assicurati che l'MFA sia abilitata per l'account «utente root»

Questo suggerimento 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 Controls v7.1 - Sub-Control 4.5 Utilizza l'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 trovano).

Utilizzo di questi framework a supporto della preparazione dell'audit

Puoi utilizzare i framework CIS AWSFoundations Benchmark v1.2 in AWS Audit Manager per prepararti per gli audit CIS. 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1	33	3	4	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0, Livello 1 e 2	45	4	4	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
				<ul style="list-style-type: none"> • AWS Security Hub

I controlli di questi framework non hanno lo scopo di verificare la conformità dei sistemi allo standard 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.

Puoi trovare questi framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Audit Manager per creare una valutazione da questi framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti dei benchmark CIS. Se è necessario modificare l'elenco dei servizi in ambito per questi framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Prerequisiti per l'utilizzo di questi framework

Molti controlli nei framework CIS AWS Foundations Benchmark v1.2 utilizzano AWS Config come tipo di origine dati. Per supportare questi controlli, devi [abilitare AWS Config](#) su tutti gli account in ciascuna Regione AWS in cui hai abilitato Audit Manager. Devi inoltre assicurarti che siano abilitate regole AWS Config specifiche e che tali regole siano configurate correttamente.

Le seguenti regole AWS Config 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.

Regola AWS Configobbligatoria	Parametri obbligatori
<u>ACCESS_KEYS_ROTATED</u>	<p>maxAccessKeyAge</p> <ul style="list-style-type: none"> • Il numero massimo di giorni senza rotazione. • Tipo: Int • Impostazione predefinita: 90 • Requisito di conformità: un massimo di 90 giorni
<u>CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED</u>	Non applicabile
<u>CLOUD_TRAIL_ENCRYPTION_ENABLED</u>	Non applicabile
<u>CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED</u>	Non applicabile
<u>CMK_BACKING_KEY_ROTATION_ENABLED</u>	Non applicabile
<u>IAM_PASSWORD_POLICY</u>	<p>MaxPasswordAge (facoltativo).</p> <ul style="list-style-type: none"> • Numero di giorni prima della scadenza della password. • Tipo: int • Impostazione predefinita: 90 • Requisito di conformità: un massimo di 90 giorni
<u>IAM_PASSWORD_POLICY</u>	<p>MinimumPasswordLength (facoltativo).</p> <ul style="list-style-type: none"> • La lunghezza minima della password. • Tipo: int • Impostazione predefinita: 14 • Requisito di conformità: minimo 14 caratteri
<u>IAM_PASSWORD_POLICY</u>	<p>PasswordReusePrevention (facoltativo).</p> <ul style="list-style-type: none"> • Numero di password prima di permettere il riutilizzo. • Tipo: int

Regola AWS Configobbligatoria	Parametri obbligatori
	<ul style="list-style-type: none"> • Impostazione predefinita: 24 • Requisito di conformità: un minimo di 24 password prima del riutilizzo
IAM_PASSWORD_POLICY	<p>RequireLowercaseCharacters (facoltativo).</p> <ul style="list-style-type: none"> • La password deve contenere almeno un carattere minuscolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un carattere minuscolo
IAM_PASSWORD_POLICY	<p>RequireNumbers (facoltativo).</p> <ul style="list-style-type: none"> • La password deve contenere almeno un numero. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un numero
IAM_PASSWORD_POLICY	<p>RequireSymbols (facoltativo).</p> <ul style="list-style-type: none"> • La password deve contenere almeno un simbolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un simbolo
IAM_PASSWORD_POLICY	<p>RequireUppercaseCharacters (facoltativo).</p> <ul style="list-style-type: none"> • La password deve contenere almeno un carattere maiuscolo. • Tipo: Booleano • Impostazione predefinita: True • Requisito di conformità: almeno un carattere maiuscolo

Regola AWS Configobbligatoria	Parametri obbligatori
<u>IAM_POLICY_IN_USE</u>	<p>policyARN</p> <ul style="list-style-type: none"> • Un ARN della policy IAM da verificare. • Tipo: string • Requisito di conformità: crea un ruolo IAM per la gestione degli incidenti con AWS. <p>policyUsageType (facoltativo).</p> <ul style="list-style-type: none"> • Specifica se si prevede che la policy venga collegata a un utente, un gruppo o un ruolo. • Tipo: string • Valori validi: IAM_USER IAM_GROUP IAM_ROLE ANY • Valore predefinito: ANY • Requisito di conformità: allega la policy di fiducia al ruolo IAM creato
<u>IAM_POLICY_NO_STAT EMENTS_WITH_ADMIN_ ACCESS</u>	Non applicabile
<u>IAM_ROOT_ACCESS_KE Y_CHECK</u>	Non applicabile
<u>IAM_USER_NO_POLICI ES_CHECK</u>	Non applicabile
<u>IAM_USER_UNUSED_CR EDENTIALS_CHECK</u>	<p>maxCredentialUsageAge</p> <ul style="list-style-type: none"> • 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
<u>INCOMING_SSH_DISABLED</u>	Non applicabile

Regola AWS Configobbligatoria	Parametri obbligatori
<u>MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS</u>	Non applicabile
<u>MULTI_REGION_CLOUD_TRAIL_ENABLED</u>	Non applicabile

Regola AWS Configobbligatoria	Parametri obbligatori
RESTRICTED_INCOMING_TRAFFIC	<p>blockedPort1 (facoltativo).</p> <ul style="list-style-type: none">• 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 <p>blockedPort2 (facoltativo).</p> <ul style="list-style-type: none">• 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 <p>blockedPort3 (facoltativo).</p> <ul style="list-style-type: none">• 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 <p>blockedPort4 (facoltativo).</p> <ul style="list-style-type: none">• 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 <p>blockedPort5 (facoltativo).</p> <ul style="list-style-type: none">• Numero di porta TCP bloccata.• Tipo: int• Impostazione predefinita: 4333

Regola AWS Configobbligatoria	Parametri obbligatori
	<ul style="list-style-type: none"> • Requisito di conformità: assicurati che nessun gruppo di sicurezza consenta l'accesso alle porte bloccate
<u>ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</u>	Non applicabile
<u>ROOT_ACCOUNT_MFA_ENABLED</u>	Non applicabile
<u>S3_BUCKET_LOGGING_ENABLED</u>	<p>targetBucket (facoltativo).</p> <ul style="list-style-type: none"> • Il bucket S3 di destinazione per l'archiviazione dei log di accesso al server. • Tipo: string • Requisito di conformità: abilita il log <p>targetPrefix (facoltativo).</p> <ul style="list-style-type: none"> • Il prefisso del bucket S3 per l'archiviazione dei log di accesso al server. • Tipo: string • Requisito di conformità: identificazione del bucket S3 per il log di CloudTrail
<u>S3_BUCKET_PUBLIC_READ_PROHIBITED</u>	Non applicabile
<u>VPC_DEFAULT_SECURITY_GROUP_CLOSED</u>	Non applicabile
<u>VPC_FLOW_LOGS_ENABLED</u>	<p>trafficType (facoltativo).</p> <ul style="list-style-type: none"> • Il <code>trafficType</code> dei log di flusso. • Tipo: string • Requisito di conformità: il log del flusso è abilitato

Altre risorse CIS

- [Il CIS AWSFoundations Benchmark v1.2.0](#)
- [Post del blog di CIS AWSFoundations Benchmark](#) sul Blog sulla sicurezza AWS

Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0

AWS Audit Manager fornisce due framework predefiniti che supportano il CIS AWSFoundations Benchmark v1.3:

- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0, Livello 1
- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0, Livello 1 e 2

Note

Per informazioni su CIS AWSFoundations Benchmark v1.2.0 e sui framework AWS Audit Manager che supportano questa versione del benchmark, consulta [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0](#).

Argomenti

- [Cos'è il CIS?](#)
- [Utilizzo di questi framework a supporto della preparazione dell'audit](#)
- [Altre risorse CIS](#)

Cos'è il CIS?

Il Center for Internet Security (CIS) ha sviluppato il [CIS AWSFoundations Benchmark](#) v1.3.0, un 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, in quanto forniscono agli utenti AWS procedure di implementazione e valutazione chiare e dettagliate.

Per ulteriori informazioni, consulta i [post del blog CIS AWSFoundations Benchmark](#) sul Blog sulla sicurezza AWS.

CIS AWSFoundations 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 Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Assicurati che l'MFA sia abilitata per l'account «utente root»

Questo suggerimento 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 Controls v7.1 - Sub-Control 4.5 Utilizza l'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 trovano).

Utilizzo di questi framework a supporto della preparazione dell'audit

Puoi utilizzare i framework CIS AWSFoundations Benchmark v1.3 in AWS Audit Manager per prepararti agli audit CIS. 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
Benchmark CIS per Amazon Web Services Foundations Benchmark v1.3.0, Livello 1	33	5	6	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
				<ul style="list-style-type: none"> • AWS Security Hub
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0, Livello 1 e 2	49	6	6	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare un elenco delle regole AWS Config utilizzate come mappature delle sorgenti dati per questi framework standard, scarica i seguenti file:

- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip](#)
- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip](#)

I controlli di questi framework non hanno lo scopo di verificare la conformità dei sistemi allo standard 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.

Puoi trovare questi framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Audit Manager per creare una valutazione da questi framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti dei benchmark CIS. Se è necessario modificare l'elenco dei servizi in ambito per questi framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse CIS

- [Post del blog di CIS AWSFoundations Benchmark](#) sul Blog sulla sicurezza AWS

Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0

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

- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0, Livello 1
- Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0, Livello 1 e 2

Note

- Per informazioni sui framework Audit Manager che supportano la versione 1.2.0, consulta [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.2.0](#).
- Per informazioni sui framework Audit Manager che supportano la versione 1.3.0, consulta [Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.3.0](#).

Argomenti

- [Cos'è il benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0?](#)
- [Utilizzo di questi framework a supporto della preparazione dell'audit](#)

- [Altre risorse CIS](#)

Cos'è il benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0?

Il benchmark CIS per CIS Amazon Web Services Foundations Benchmark, v1.4.0, Livello 1 e 2 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 Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Assicurati che l'MFA sia abilitata per l'account «utente root»

Questo suggerimento 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 Controls v7.1 - Sub-Control 4.5 Utilizza l'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

Puoi utilizzare i framework CIS AWSFoundations Benchmark v1.4.0 per prepararti 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
Benchmark CIS per CIS Amazon Web Services	32	6	7	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Foundations Benchmark v1.4.0, Livello 1				<ul style="list-style-type: none"> • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
Benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0, Livello 1 e 2	50	8	7	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare un elenco delle regole AWS Config utilizzate come mappature delle sorgenti dati per questi framework standard, scarica i seguenti file:

- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip](#)
- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip](#)

I controlli in questi framework non hanno lo scopo di verificare la conformità dei sistemi allo standard del benchmark CIS per CIS Amazon Web Services Foundations Benchmark v1.4.0. 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.

Puoi trovare questi framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questi framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Audit Manager per creare una valutazione da questi framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti dei benchmark CIS. Se è necessario modificare l'elenco dei servizi in ambito per questi framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questi framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse CIS

- [Benchmark CIS](#) del Center for Internet Security
- [Post del blog di CIS AWS Foundations Benchmark](#) sul Blog sulla sicurezza AWS

Gruppo di implementazione 1 di CIS Controls v7.1

AWS Audit Manager fornisce un framework standard predefinito che supporta il gruppo di implementazione 1 del Center for Internet Security (CIS) Controls v7.1.

Note

Per informazioni su CIS Controls v8 IG1 e sul framework AWS Audit Manager che supporta questo standard, consulta [Gruppo di implementazione 1 di CIS Controls v8](#).

AWS Audit Manager fornisce un framework predefinito che supporta il Center for Internet Security (CIS) per facilitare la preparazione degli audit.

Argomenti

- [Cosa sono i controlli CIS?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse CIS](#)

Cosa sono i controlli CIS?

I controlli CIS sono un insieme di azioni prioritarie che, collettivamente, costituiscono un insieme di best practice per una difesa approfondita. 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 Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assicurati che l'MFA sia abilitata per l'account «utente root».
 - Questo suggerimento 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 Controls v7.1 - Sub-Control 4.5 Utilizza l'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 a supporto della preparazione dell'audit

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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
Controlli CIS v7.1 IG1	21	22	16	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip](#).

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.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti dei controlli CIS. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse CIS

- [Controlli CIS v7.1 IG1](#)

Gruppo di implementazione 1 di CIS Controls v8

AWS Audit Manager fornisce un framework standard predefinito che supporta il gruppo di implementazione 1 del Center for Internet Security (CIS) Controls v8.

Note

Per informazioni su CIS Controls v7.1 IG1 e sul framework AWS Audit Manager che supporta questo standard, consulta [Gruppo di implementazione 1 di CIS Controls v7.1](#).

Argomenti

- [Cosa sono i controlli CIS?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse CIS](#)

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. L'aggiornamento è scaturito da fattori quali il passaggio al cloud computing, virtualizzazione, mobilità, outsourcing, lavoro da casa e cambiamento delle tattiche degli aggressori. 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 Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assicurati che l'MFA sia abilitata per l'account «utente root».
 - Questo suggerimento 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 Controls v7.1 - Sub-Control 4.5 Utilizza l'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 a supporto della preparazione dell'audit

Puoi utilizzare il framework Controlli CIS v8 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework CIS Controls 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 CIS Controls v8 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
CIS Controls v8 IG1	25	31	15	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip](#).

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.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti dei controlli CIS. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse CIS

- [CIS Controls v8](#)

FedRAMP Moderate Baseline

AWS Audit Manager fornisce un framework FedRAMP Moderate Baseline per facilitare la preparazione degli audit.

Argomenti

- [Cos'è FedRAMP?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse FedRAMP](#)

Cos'è FedRAMP?

Il Federal Risk and Authorization Management Program (FedRAMP) è stato istituito 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 a supporto della preparazione dell'audit

Puoi utilizzare il framework FedRAMP Moderate Baseline 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 FedRAMP. 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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
FedRAMP Moderate Baseline	303	908	325	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip](#).

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi a FedRAMP. 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.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti della FedRAMP Moderate Baseline. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse FedRAMP

- [Pagina di conformità AWS per FedRAMP](#)
- [Post del blog FedRAMP AWS](#)

Regolamento generale sulla protezione dei dati (GDPR)

AWS Audit Manager fornisce un framework standard predefinito che supporta il Regolamento generale sulla protezione dei dati (GDPR). Per impostazione predefinita, 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 funzione di controllo personalizzato in AWS Audit Manager. Per ulteriori informazioni, consulta [Utilizzo di questo framework a supporto della preparazione dell'audit](#).

Argomenti

- [Cos'è il Regolamento generale sulla protezione dei dati \(GDPR\)?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse sul GDPR](#)

Cos'è il Regolamento generale sulla protezione dei dati (GDPR)?

Il Regolamento generale sulla protezione dei dati (GDPR) è una nuova 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 AWS Audit Manager. Per ulteriori informazioni, consulta il [Centro generale sulla protezione dei dati \(GDPR\)](#).

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework GDPR in AWS 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	Servizi AWS nell'ambito di applicazione
GDPR	0	371	10	Nessuno

Puoi trovare il framework GDPR nella scheda Framework standard della [Libreria Framework](#) di Audit Manager. Dal momento che il framework standard contiene solo controlli manuali, nessun Servizio AWS rientra nell'ambito di applicazione.

Note

Se desideri automatizzare la raccolta di prove per il GDPR, puoi utilizzare Audit Manager per [creare controlli personalizzati](#) per il GDPR. La tabella seguente fornisce suggerimenti sulle origini dati AWS 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 suggerimenti utilizzano AWS Config e AWS Security Hub come origini dati. Per raccogliere prove con successo da queste origini dati, assicurati di eseguire la seguente procedura:

- Conferma di aver seguito le istruzioni per l'[attivazione e la configurazione di AWS Config e AWS Security Hub](#) nel tuo Account AWS.
- Conferma di aver incluso AWS Config e Security Hub come servizi nell'ambito di applicazione. Per esaminare l'elenco dei servizi oggetto della valutazione, consulta la scheda [Servizi AWS Revisione di una valutazione](#). Per modificare questo elenco, consulta [Modifica di Servizi AWS nell'ambito di applicazione](#).

Dopo aver configurato entrambi i servizi in questo modo, Audit Manager raccoglie le prove ogni volta che viene effettuata una valutazione per la regola AWS Config specificata o il controllo del Security Hub.

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 25 Protezione e dei dati fin dalla progettazione e per impostazione predefinita.1</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale • Bucket AWS CloudTrail non pubblico • Mostra tutte le policy con un Allow: *:* ed elenca tutti i principali e i servizi che utilizzano tali policy <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati:</p>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none">• 1.1 (CloudWatch.1)• 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)• 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)

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none">• 3.10 (CloudWatch.10)• 3.11 (CloudWatch.11)• 3.12 (CloudWatch.12)• 3.13 (CloudWatch.13)• 3.14 (CloudWatch.14)• Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 25 Protezione e dei dati fin dalla progettazione e per impostazione predefinita.2</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale • Bucket AWS CloudTrail non pubblico • Mostra tutte le policy con un <code>Allow: * : *</code> ed elenca tutti i principali e i servizi che utilizzano tali policy <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati:</p> <ul style="list-style-type: none"> • 1.1 (CloudWatch.1) • 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
		<ul style="list-style-type: none"> • 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 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

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
<p>Articolo 25 Protezione e dei dati fin dalla progettazione e per impostazione predefinita.3</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale • Bucket AWS CloudTrail non pubblico • Mostra tutte le policy con un <code>Allow: * : *</code> ed elenca tutti i principali e i servizi che utilizzano tali policy <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Scegli AWS Security Hub come tipo di origine dati e seleziona i seguenti controlli del Security Hub come mappature dell'origine dati:</p> <ul style="list-style-type: none"> • 1.1 (CloudWatch.1) • 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
		<ul style="list-style-type: none">• 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 (CloudWatch.10)• 3.11 (CloudWatch.11)• 3.12 (CloudWatch.12)• 3.13 (CloudWatch.13)• 3.14 (CloudWatch.14)

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
Articolo 30 Registrazione delle attività di trattamento.1	Capitolo 4 - Titolare e responsabile del trattamento	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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 <p>Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo del Security Hub come mappatura dell'origine dati:</p> <ul style="list-style-type: none"> • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 30</p> <p>Registrazione delle attività di trattamento.2</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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 <p>Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo del Security Hub come mappatura dell'origine dati:</p> <ul style="list-style-type: none"> • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 30 Registrazione delle attività di trattamento.3</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale • Bucket AWS CloudTrail non pubblico • Mostra tutte le policy con un Allow: *:* ed elenca tutti i principali e i servizi che utilizzano tali policy <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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 <p>Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo del Security Hub come mappatura dell'origine dati:</p> <ul style="list-style-type: none"> • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 30</p> <p>Registrazione delle attività di trattamento.4</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale • Bucket AWS CloudTrail non pubblico • Mostra tutte le policy con un Allow: *:* ed elenca tutti i principali e i servizi che utilizzano tali policy <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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 <p>Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo del Security Hub come mappatura dell'origine dati:</p> <ul style="list-style-type: none"> • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 30 Registrazione delle attività di trattamento.5</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • Mostra tutti gli eventi dell'account root in un arco temporale <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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 <p>Scegli AWS Security Hub come tipo di origine dati e seleziona il seguente controllo del Security Hub come mappatura dell'origine dati:</p> <ul style="list-style-type: none"> • Config.1

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 32 Sicurezza del trattamento.1</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • 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 ritto grafato a riposo. • Avvisi Amazon CloudWatch per AWS Config che visualizzano tutte le modifiche e tutte le impostazioni commentate • Tutte le attività root <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • <u>RDS_STORAGE_ENCRYPTED</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none">• <u>API_GW_CACHE_ENABLED_AND_ENCRYPTED</u>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 32 Sicurezza del trattamento.2</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • 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 rittoografato a riposo. • Avvisi Amazon CloudWatch per AWS Config che visualizzano tutte le modifiche e tutte le impostazioni commentate • Tutte le attività root <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • <u>RDS_STORAGE_ENCRYPTED</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none"><li data-bbox="464 260 1205 296">• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 32 Sicurezza del trattamento.3</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • 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 ritrattografato a riposo. • Avvisi Amazon CloudWatch per AWS Config che visualizzano tutte le modifiche e tutte le impostazioni commentate • Tutte le attività root <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • <u>RDS_STORAGE_ENCRYPTED</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none"><li data-bbox="467 260 1203 296">• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
<p>Articolo 32 Sicurezza del trattamento.4</p>	<p>Capitolo 4 - Titolare e responsabile del trattamento</p>	<p>Puoi creare un controllo personalizzato in AWS Audit Manager che supporti questo controllo GDPR.</p> <p>Quando specifichi i dettagli del controllo, inserisci quanto segue nella sezione Informazioni sul test:</p> <ul style="list-style-type: none"> • 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 ritrattografato a riposo. • Avvisi Amazon CloudWatch per AWS Config che visualizzano tutte le modifiche e tutte le impostazioni commentate • Tutte le attività root <p>Quando configuri le origini dati di controllo, ti consigliamo di includere tutte le seguenti origini dati:</p> <p>Scegli AWS Config come tipo di origine dati e seleziona le seguenti regole gestite AWS Config come mappature delle origini dati:</p> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • <u>RDS_STORAGE_ENCRYPTED</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nome del controllo:	Set di controllo	Mappatura dell'origine dati di controllo consigliata
		<ul style="list-style-type: none">• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Dopo aver creato i nuovi controlli personalizzati per il GDPR, puoi aggiungerli a un framework GDPR personalizzato. Per ulteriori informazioni, consulta [Creazione di un framework personalizzato](#) e [Modifica di un framework personalizzato](#). È possibile creare una valutazione dal framework GDPR personalizzato. In questo modo, AWS Audit Manager può raccogliere automaticamente prove per i controlli personalizzati che hai aggiunto. Per istruzioni su come creare una valutazione utilizzando un framework, consulta [Creazione di una valutazione](#).

Altre risorse sul GDPR

- [Centro per il Regolamento generale sulla protezione dei dati \(GDPR\)](#)
- [Post sul blog sul GDPR AWS](#)

Gramm-Leach-Bliley Act

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

Argomenti

- [Cos'è il Gramm-Leach-Bliley Act \(GLBA\)?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)

Cos'è il Gramm-Leach-Bliley Act (GLBA)?

Il Gramm-Leach-Bliley Act (GLB Act o GLBA), 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 a supporto della preparazione dell'audit

Puoi utilizzare il framework Gramm-Leach-Bliley Act (GLBA) 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 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 Audit Manager e iniziare a raccogliere prove rilevanti per un audit GLBA. Nella valutazione, puoi specificare gli Account AWS e i servizi che desideri includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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 GLBA sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Gramm-Leach-Bliley Act (GLBA)	4	110	16	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_GLBA.zip](#).

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

Puoi trovare il framework GLBA nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del GLBA. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

GxP 21 CFR parte 11

AWS Audit Manager fornisce un framework predefinito che supporta le normative GxP CFR parte 11 basate sulle best practice AWS.

Note

Per informazioni su GxP UE Allegato 11 e sul framework Audit Manager che lo supporta, vedere [GxP UE Allegato 11](#).

Argomenti

- [Cos'è GxP CFR parte 11?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse GxP](#)

Cos'è GxP CFR parte 11?

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.

Il termine GxP comprende un'ampia gamma di attività relative alla conformità. Tra esse figurano buone pratiche di laboratorio (GLP), buone pratiche cliniche (GCP) e buone prassi di fabbricazione (GMP). Ciascuno di questi diversi tipi di attività comporta requisiti specifici di prodotto che le organizzazioni delle scienze della vita devono implementare. Essi si basano sul tipo di prodotti fabbricati dalle organizzazioni e dal paese in cui vengono venduti i loro prodotti. Quando le organizzazioni del settore delle scienze biologiche utilizzano sistemi computerizzati per eseguire determinate attività GxP, sono tenute a garantire che il sistema informatizzato GxP sia sviluppato, convalidato e utilizzato in modo appropriato per l'uso previsto del sistema.

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

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework GxP 21 CFR Parte 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 GxP. 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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. Lo fa sulla base dei controlli definiti nel framework GxP 21 CFR Parte 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 GxP CFR Parte 11 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
GxP 21 CFR Parte 11	13	14	7	<ul style="list-style-type: none"> • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip](#).

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è

preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework GxP CFR Part 11. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse GxP

- [Pagina sulla conformità AWSper GxP](#)
- [Considerazioni sull'utilizzo dei prodotti AWSnei sistemi GxP](#)

GxP UE Allegato 11

AWS Audit Manager fornisce un framework predefinito che supporta le normative GxP UE Allegato 11 basate sulle best practice AWS.

Note

Per informazioni su GxP 21 CFR Parte 11 e sul framework Audit Manager che lo supporta, consulta [GxP 21 CFR parte 11](#).

Argomenti

- [Cos'è GxP UE Allegato 11](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)

Cos'è GxP UE Allegato 11

Il framework GxP UE Allegato 11 è l'equivalente europeo del framework FDA 21 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 distanti dalla FDA (21 CFR Part 11). L'allegato 11 definisce i criteri per la gestione dei record elettronici e delle firme elettroniche.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework GxP UE Allegato 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 GxP. 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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework GxP UE Allegato 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 GxP UE Allegato 11 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
GxP UE Allegato 11	19	13	3	<ul style="list-style-type: none"> • Amazon CloudWatch • AWS CloudTrail • AWS Config

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
				<ul style="list-style-type: none"> • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip](#).

I controlli di questo framework non hanno lo scopo di verificare la conformità dei sistemi ai requisiti del GxP UE Allegato 11. Inoltre, non possono garantire il superamento di un audit GxP. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework GxP UE Allegato 11. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Norma di sicurezza Health Insurance Portability and Accountability Act (HIPAA) 2003

AWS Audit Manager fornisce un framework predefinito che supporta le regole HIPAA per facilitare la preparazione degli audit.

Note

Questo framework era precedentemente denominato HIPAA nella libreria del framework. L'8 marzo 2023, abbiamo aggiornato il nome di questo framework in Norma di sicurezza HIPAA 2003 per differenziarlo dalla Norma di sicurezza Omnibus finale HIPAA 2013.

Per informazioni sulla norma di sicurezza Omnibus finale HIPAA 2013 e sul framework Audit Manager che supporta questo standard, consulta [Norma di sicurezza Omnibus finale Health Insurance Portability and Accountability Act \(HIPAA\) 2013](#).

Argomenti

- [Cosa sono l'HIPAA e la norma di sicurezza HIPAA 2003?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse HIPAA](#)

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

L'Health Insurance Portability and Accountability and Accountability and Portability and Accountability Act statunitense del 1996 (HIPAA) è una legislazione che aiuta i lavoratori statunitensi a mantenere la copertura assicurativa sanitaria in caso di cambiamento o di perdita del 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 operatori sanitari, contribuenti e professionisti IT utilizzano servizi cloud AWS basati su utilità per elaborare, archiviare e trasmettere informazioni sanitarie protette (PHI). AWS consente alle entità e ai partner coinvolti soggetti a HIPAA di utilizzare l'ambiente sicuro AWS per l'elaborazione, la conservazione e l'archiviazione delle informazioni sanitarie protette.

Per istruzioni su come utilizzare AWS per l'elaborazione e l'archiviazione di informazioni sanitarie, consulta il whitepaper [Architecting for HIPAA Security and Compliance on Amazon Web Services](#).

Utilizzo di questo framework a supporto della preparazione dell'audit

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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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 della Norma di sicurezza HIPAA 2003 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Norma di sicurezza HIPAA 2003	35	53	5	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip](#).

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai

requisiti del framework HIPAA. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse HIPAA

- [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](#)
- [Pagina di conformità AWS per l'HIPAA](#)

Norma di sicurezza Omnibus finale Health Insurance Portability and Accountability Act (HIPAA) 2013

AWS Audit Manager fornisce un framework predefinito che supporta le regole HIPAA per facilitare la preparazione degli audit.

Note

Per informazioni sulla norma di sicurezza HIPAA 2003 e sul framework AWS Audit Manager che supporta questo standard, consulta [Norma di sicurezza Health Insurance Portability and Accountability Act \(HIPAA\) 2003](#).

Argomenti

- [Cosa sono l'HIPAA e la norma di sicurezza Omnibus finale HIPAA?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse HIPAA](#)

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

L'Health Insurance Portability and Accountability and Accountability and Portability and Accountability Act statunitense del 1996 (HIPAA) è una legislazione che aiuta i lavoratori statunitensi a mantenere la copertura assicurativa sanitaria in caso di cambiamento o di perdita del 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 operatori sanitari, contribuenti e professionisti IT utilizzano servizi cloud AWS basati su utilità per elaborare, archiviare e trasmettere informazioni sanitarie protette (PHI). AWS consente alle entità e ai partner coinvolti soggetti a HIPAA di utilizzare l'ambiente sicuro AWS per l'elaborazione, la conservazione e l'archiviazione delle informazioni sanitarie protette. Per istruzioni su come utilizzare AWS per l'elaborazione e l'archiviazione di informazioni sanitarie, consulta il whitepaper [Architecting for HIPAA Security and Compliance on Amazon Web Services](#).

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework della Norma di sicurezza Omnibus finale HIPAA 2013 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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 della norma di sicurezza Omnibus finale HIPAA 2013 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Norma di sicurezza Omnibus finale HIPAA 2013	39	46	5	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip](#).

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework HIPAA. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse HIPAA

- [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](#)
- [Pagina di conformità AWS per l'HIPAA](#)

ISO/IEC 27001:2013 Allegato A

AWS Audit Manager fornisce un framework standard predefinito che struttura e automatizza le valutazioni per lo standard ISO/IEC 27001:2013 Allegato A.

Argomenti

- [Che cos'è lo standard ISO/IEC 27001:2013 Allegato A?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse dello standard ISO/IEC 27001:2013 Allegato A.](#)

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, non governative e senza scopo di lucro che sviluppano e pubblicano standard internazionali interamente basati sul consenso.

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 a supporto della preparazione dell'audit

Puoi utilizzare il framework AWS Audit Manager dello standard ISO/IEC 27001:2013 Allegato A 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 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 Audit Manager e iniziare a raccogliere prove rilevanti per un audit dello standard ISO/IEC 27001:2013 Allegato A. Nella valutazione, puoi specificare gli Account AWS e i servizi che desideri includere nell'ambito dell'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
ISO-IEC 27001:2013 Allegato A	50	64	35	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

 Tip

Per esaminare le regole AWS Config utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip](#).

I controlli di questi framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi a questo standard internazionale. Inoltre, non possono garantire il superamento di 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 [Libreria Framework](#) di Audit Manager.

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework dello standard ISO/IEC 27001:2013 Allegato A. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#). Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse dello standard ISO/IEC 27001:2013 Allegato A.

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

NIST 800-53 (Rev. 5) Low-Moderate-High

AWS Audit Manager fornisce un framework predefinito che struttura e automatizza le valutazioni per lo standard di conformità NIST 800-53, sulla base delle best practice AWS.

Note

- Per informazioni sui framework Audit Manager che supportano NIST 800-171, consulta [NIST SP 800-171 \(Rev. 2\)](#).
- Per informazioni sui framework Audit Manager che supportano il Framework NIST per la sicurezza informatica, consulta [Framework NIST per la sicurezza informatica versione 1.1](#).

Argomenti

- [Che cos'è lo standard NIST 800-53?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse del NIST](#)

Che cos'è lo standard NIST 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 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 800-53 (Rev. 5) Low-Moderate-High 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 a supporto della preparazione dell'audit

Puoi utilizzare il framework NIST 800-53 (Rev. 5) Low-Moderate-High 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 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. Lo fa sulla base dei controlli definiti nel framework NIST 800-53 (Rev. 5) Low-Moderate-High. 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 NIST 800-53 (Rev. 5) Low-Moderate-High sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
NIST 800-53 (Rev. 5) Low-Moderate-High	225	782	280	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

 Tip

Per esaminare le regole AWS Config utilizzate come mappature delle sorgenti dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip](#).

I controlli di questi framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi allo standard NIST. 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.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework NIST 800-53 (Rev. 5) Low-Moderate-High. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse del NIST

- [National Institute of Standards and Technology \(NIST\)](#)
- [Centro risorse per la sicurezza informatica NIST](#)
- [AWSPagina di conformità per il NIST](#)

Framework NIST per la sicurezza informatica versione 1.1

AWS Audit Manager fornisce un framework predefinito che struttura e automatizza le valutazioni per il framework NIST per la sicurezza informatica, sulla base delle best practice. AWS

Note

- Per informazioni sui framework Audit Manager che supportano NIST 800-53 (Rev. 5) Low-Moderate-High, consulta [NIST 800-53 \(Rev. 5\) Low-Moderate-High](#).
- Per informazioni sui framework Audit Manager che supportano NIST SP 800-171 (Rev. 2), consulta [NIST SP 800-171 \(Rev. 2\)](#).

Argomenti

- [Cos'è il framework NIST per la sicurezza informatica?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)

- [Altre risorse del NIST](#)

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 a supporto della preparazione dell'audit

Puoi utilizzare il framework NIST per la sicurezza informatica versione 1.1 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 NIST CSF. Al momento, Audit Manager supporta il componente principale del framework e offre 56 controlli automatici e 52 controlli

manuali. Questi controlli corrispondono a 23 categorie di sicurezza informatica definite nei principi fondamentali del framework. Audit Manager non supporta il profilo e i componenti di implementazione in questo framework.

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 l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. La valutazione avviene sulla base dei controlli definiti nel framework NIST per la sicurezza informatica versione 1.1. 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 NIST per la sicurezza informatica versione 1.1 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
Framework NIST per la sicurezza informatica versione 1.1	56	52	23	<ul style="list-style-type: none"> • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip](#).

I controlli offerti da Audit Manager non hanno lo scopo di verificare la conformità dei sistemi al framework NIST per la sicurezza informatica. Inoltre, non possono garantire il superamento di un audit di sicurezza informatica NIST. AWS Audit Manager non verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework NIST per la sicurezza informatica versione 1.1. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse del NIST

- [National Institute of Standards and Technology \(NIST\)](#)
- [Centro risorse per la sicurezza informatica NIST](#)
- [AWS Pagina di conformità per il NIST](#)
- [Framework NIST per la sicurezza informatica: allineamento al NIST CSF nel cloud AWS](#)

NIST SP 800-171 (Rev. 2)

AWS Audit Manager fornisce un framework predefinito che struttura e automatizza le valutazioni per lo standard di conformità NIST SP 800-171 sulla base delle best practice AWS.

Note

- Per informazioni sui framework Audit Manager che supportano NIST 800-53 (Rev. 5) Low-Moderate-High, consulta [NIST 800-53 \(Rev. 5\) Low-Moderate-High](#).
- Per informazioni sui framework Audit Manager che supportano il Framework NIST per la sicurezza informatica versione 1.1, consulta [Framework NIST per la sicurezza informatica versione 1.1](#).

Argomenti

- [Che cos'è lo standard NIST SP 800-171?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse del NIST](#)

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. Il NIST 800-171 è stato sottoposto ad 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 800-171 salvaguardano le informazioni non classificate controllate (CUI) nelle reti IT degli appaltatori e dei 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 800-171 si applica solo alle parti della rete di un appaltatore in cui sono presenti le CUI.

Utilizzo di questo framework a supporto della preparazione dell'audit

Puoi utilizzare il framework NIST SP 800-171 Rev. 2 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 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. Lo fa sulla base dei controlli definiti nel framework NIST SP 800-171 Rev. 2. 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 NIST SP 800-171 Rev. 2 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
NIST SP 800-171 Rev. 2	66	58	16	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip](#).

I controlli di questi framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi allo standard NIST 800-171. Inoltre, non possono garantire il superamento di un audit NIST. AWS Audit Manager verifica automaticamente i controlli procedurali che richiedono la raccolta manuale delle prove.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per informazioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework NIST SP 800-171 Rev. 2. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse del NIST

- [National Institute of Standards and Technology \(NIST\)](#)
- [Centro risorse per la sicurezza informatica NIST](#)
- [AWSPagina di conformità per il NIST](#)

PCI DSS V3.2.1

AWS Audit Manager fornisce un framework predefinito che supporta 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](#)
- [Altre risorse PCI DSS](#)

Che cos'è PCI DSS?

Il Payment Card Industry Data Security Standard (PCI DSS) è uno standard di tutela delle informazioni proprietario gestito dal PCI Security Standards Council. È amministrato dal [PCI Security Standards Council](#), fondato da American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. Lo standard PCI DSS si applica alle entità che archiviano, elaborano o trasmettono dati dei titolari di carta (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 di livello 1 PCI DSS, che è 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'Attestazione di conformità allo standard PCI DSS (AOC) e il riepilogo delle responsabilità sono disponibili su AWS Artifact. Si tratta di un portale self-service per l'accesso su richiesta ai report di conformità AWS. Accedi a [AWS Artifact nella console di gestione AWS](#) o scopri di più nella sezione [Nozioni di base su 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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 PCI DSS V3.2.1 sono i seguenti:

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
PCI DSS V3.2.1	175	487	12	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip](#).

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per informazioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework PCI DSS V3.2.1. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse PCI DSS

- [PCI Security Standards Council](#)
- [Libreria dei documenti del PCI Security Standards Council](#).
- [AWSPagina di conformità per PCI DSS](#)

PCI DSS V4.0

AWS Audit Manager fornisce un framework predefinito che supporta lo standard PCI DSS (Payment Card Industry Data Security Standard) 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?](#)
- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse PCI DSS](#)

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.

Per ulteriori informazioni sulle modifiche, consulta il [Riepilogo delle modifiche di PCI DSS dalla versione 3.2.1 a 4.0](#).

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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
PCI DSS v4.0	152	128	15	<ul style="list-style-type: none"> • Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Servizio OpenSearch di Amazon • Amazon Redshift

Nome del framework in AWS Audit Manager	Numero di controlli automatici	Numero di controlli manuali	Numero di set di controllo	Servizi AWS nell'ambito di applicazione
				<ul style="list-style-type: none"> • Amazon Relational Database Service • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

 Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica il file [AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip](#).

I controlli di questi framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi allo standard PCI DSS. Inoltre, non possono garantire il superamento di un audit PCI DSS.

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

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per informazioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti del framework PCI DSS V4. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse PCI DSS

- [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](#)
- [Payment Card Industry Data Security Standard \(PCI DSS\) v4.0 nella Guida alla conformità di AWS](#)
- [Riepilogo delle modifiche di PCI DSS dalla versione 3.2.1 a 4.0](#)

SOC 2

SOC 2 è una procedura di audit che garantisce la gestione sicura dei dati di un'azienda. AWS Audit Manager fornisce un framework predefinito che supporta SOC 2.

Argomenti

- [Che cos'è SOC 2?](#)

- [Utilizzo di questo framework a supporto della preparazione dell'audit](#)
- [Altre risorse SOC 2](#)

Che cos'è SOC 2?

System and Organization Controls (SOC), 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.

I report SOC AWS sono report di valutazione di terze parti che documentano in che modo AWS consegue i controlli e gli obiettivi chiave di conformità. Lo scopo di questi report è consentire a clienti e revisori di raccogliere informazioni sui controlli previsti da AWS per supportare operatività e compliance. Esistono cinque report SOC AWS:

- Report SOC 1 AWS, disponibile per i clienti AWS da [AWS Artifact](#).
- Report SOC 2 AWS su sicurezza, disponibilità e riservatezza, disponibile per i clienti AWS da [AWS Artifact](#).
- Report SOC 2 AWS su sicurezza, disponibilità e riservatezza, disponibile per i clienti AWS da [AWS Artifact](#) (l'ambito di applicazione comprende solo Amazon DocumentDB).
- Report SOC 2 AWS sulla privacy di tipo I, disponibile per i clienti AWS da [AWS Artifact](#).
- Report SOC 3 AWS 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 Audit Manager e iniziare a raccogliere prove rilevanti per l'audit. Dopo aver creato una valutazione, Audit Manager inizia a valutare le tue risorse AWS. 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	Servizi AWS nell'ambito di applicazione
SOC 2	20	41	20	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

 Tip

Per esaminare le regole AWS Config utilizzate come mappature delle origini dati in questo framework standard, scarica [AuditManager_ConfigDataSourceMappings_SOC2.zip](#)

I controlli di questo framework AWS Audit Manager non hanno lo scopo di verificare la conformità dei sistemi. 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.

Puoi trovare il framework nella scheda Framework standard della [Libreria Framework](#) di Audit Manager.

Per istruzioni su come creare una valutazione utilizzando questo framework, consulta [Creazione di una valutazione](#).

Quando utilizzi la console Gestione audit per creare una valutazione da questo framework standard, per impostazione predefinita l'elenco dei Servizi AWS all'interno dell'ambito di applicazione è preselezionato e non può essere modificato. Questo perché Gestione audit mappa e seleziona automaticamente le origini dati e i servizi per l'utente. Questa selezione viene effettuata in base ai requisiti SOC 2. Se è necessario modificare l'elenco dei servizi in ambito per questo framework, è possibile farlo utilizzando le operazioni API [CreateAssessment](#) o [UpdateAssessment](#). In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Per istruzioni su come personalizzare questo framework per supportare requisiti specifici, consulta [Personalizzazione di un framework esistente](#) e [Personalizzazione di un controllo esistente](#).

Altre risorse SOC 2

- [Pagina sulla conformità AWS per SOC](#)

Libreria di controllo

È possibile accedere e gestire i controlli dalla libreria di controllo in Audit Manager. È possibile accedere alla libreria di controllo in qualsiasi momento selezionando libreria di controllo nel riquadro di navigazione della console Audit Manager.

La libreria di controllo contiene un catalogo di controlli standard e controlli personalizzati.

- I controlli standard sono controlli predefiniti forniti da AWS. È possibile visualizzare i dettagli di configurazione dei controlli standard, ma non modificarli o eliminarli. Tuttavia, puoi personalizzare qualsiasi controllo standard per crearne uno nuovo che soddisfi i tuoi requisiti specifici.
- I controlli personalizzati sono controlli personalizzati che possiedi e definisci. Con un controllo personalizzato, puoi specificare da quali origini dati desideri raccogliere prove. È quindi possibile aggiungere controlli personalizzati a un framework personalizzato.

Per ulteriori informazioni su come aggiungere un controllo personalizzato a un framework personalizzato, consulta [Libreria Framework](#). Per ulteriori informazioni su come creare una valutazione da un framework Audit Manager, consulta [Valutazioni in AWS Audit Manager](#).

Questa sezione descrive come creare e gestire controlli personalizzati in Audit Manager.

Argomenti

- [Accesso ai controlli disponibili in AWS Audit Manager](#)
- [Revisione dei dettagli di un controllo](#)
- [Creazione di un controllo personalizzato](#)
- [Modifica di un controllo personalizzato](#)
- [Eliminazione di un controllo personalizzato](#)
- [Modifica della frequenza di raccolta delle prove per un controllo](#)
- [Fonti di dati di controllo supportate per prove automatizzate](#)

Accesso ai controlli disponibili in AWS Audit Manager

È possibile visualizzare tutti i controlli disponibili nella pagina della libreria di controllo nella console Audit Manager. Da qui, puoi anche [creare un controllo personalizzato](#) o [personalizzare un controllo esistente](#).

Puoi anche visualizzare tutti i controlli disponibili utilizzando l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare i controlli disponibili (console)

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Scegli Libreria di controllo nel riquadro di navigazione.
3. Scegli la scheda Controlli standard o la scheda Controlli personalizzati per sfogliare i controlli disponibili.
4. Per visualizzare i dettagli di un controllo, selezionare il nome del controllo.

AWS CLI

Per visualizzare i controlli disponibili (AWS CLI)

Esegui il comando [list-controls](#) e specifica un `--control-type`. In entrambi i casi, è possibile recuperare un elenco di controlli standard. In alternativa, puoi recuperare un elenco di controlli personalizzati.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Per visualizzare i controlli disponibili (API)

Utilizzate l'[ListControls](#) operazione e specificate un [ControlType](#). In entrambi i casi, puoi restituire un elenco di controlli standard. In alternativa, puoi restituire un elenco di controlli 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'`ListControls` operazione e i parametri in uno degli SDK specifici della lingua AWS .

Revisione dei dettagli di un controllo

È possibile esaminare i dettagli di un controllo utilizzando la console Audit Manager, l'API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Per visualizzare i dettagli del controllo (console)

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione, scegliere libreria di controllo per visualizzare un elenco di controlli disponibili.
3. Scegli la scheda Controlli standard o la scheda Controlli personalizzati per sfogliare i controlli disponibili.
4. Per visualizzare i dettagli di un controllo, seleziona il nome del controllo.

Quando apri un controllo, viene visualizzata una pagina dei dettagli di controllo. Le sezioni di questa pagina e i relativi contenuti sono descritti di seguito.

Sezione riepilogo

In questa sezione viene fornita una panoramica del controllo. Include le seguenti informazioni:

- Nome del controllo: il nome del controllo.
- Tipo di controllo: specifica se il controllo è un controllo standard o personalizzato.
- Tag: il numero di tag associati al controllo.
- Tipi di origini dati: il numero di [tipi di origini dati](#) utilizzati per questo controllo.
- Mappature: il numero di attributi di [mappatura](#) utilizzati per recuperare dati da un'origine dati.

Se stai visualizzando un controllo personalizzato, vengono visualizzati anche i seguenti dettagli:

- Creato da: l'account che ha creato il controllo personalizzato.
- Data di creazione: la data in cui è stato creato il controllo personalizzato.
- Ultimo aggiornamento: la data dell'ultima modifica apportata al controllo personalizzato.

Scheda Dettagli

In questa scheda viene fornita una panoramica di base del controllo. Include le seguenti informazioni:

- La sezione Descrizione fornisce una descrizione del controllo.
- La sezione Informazioni sui test fornisce una descrizione delle procedure di test consigliate per il controllo.
- La sezione relativa al Piano di azione descrive le azioni consigliate da eseguire se è necessario porre rimedio al controllo.

Scheda origini dati

In questa scheda vengono visualizzate le informazioni sulle origini dei dati per il controllo. Include le seguenti informazioni:

- Nome dell'origine dati: si applica solo ai controlli personalizzati. Si riferisce al nome descrittivo che hai assegnato a ciascuna fonte di dati. Puoi usare questo nome per distinguere tra più origini dati che rientrano nello stesso tipo di origine dati.
- Tipo di origine dati: specifica da dove provengono i dati relativi alle prove.
 - Se Audit Manager raccoglie le prove, l'origine dati può essere di quattro tipi: AWS Security Hub, AWS Config, AWS CloudTrail, o AWS chiamate API.
 - Se carichi le tue prove, il tipo di origine dati è Manuale. Una descrizione indica se la prova manuale richiesta è un caricamento di file o una risposta testuale.
- Mappatura: questo è l'attributo di mappatura utilizzato per identificare e recuperare i dati dalla fonte dei dati.
 - Se il tipo di origine dati è AWS Config, la mappatura è il nome di una AWS Config regola specifica (ad esempio, `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager utilizza questa mappatura per riportare il risultato del controllo delle regole direttamente da AWS Config.
 - Se il tipo di origine dati è AWS Security Hub, la mappatura è il nome di un controllo specifico del Security Hub (ad esempio, `1.1 - Avoid the use of the "root" account`). Audit Manager utilizza questa mappatura per riportare il risultato del controllo di sicurezza direttamente dal Security Hub.
 - Se il tipo di origine dati sono chiamate AWS API, la mappatura è il nome di una chiamata API specifica (ad esempio, `ec2_DescribeSecurityGroups`). Audit Manager utilizza questa mappatura per raccogliere la risposta dell'API.

- Se l'origine dati è AWS CloudTrail, la mappatura è il nome di un CloudTrail evento specifico (ad esempio, `CreateAccessKey`). Audit Manager utilizza questa mappatura per raccogliere l'attività utente correlata dai CloudTrail registri.
- Frequenza: specifica la frequenza con cui Audit Manager raccoglie prove dalla fonte dei dati. La frequenza varia a seconda del tipo di origine dati. Per ulteriori informazioni, scegli il valore nella colonna o consulta [Frequenza di raccolta delle prove](#).

Scheda Tag

In questa scheda vengono elencati i tag associati al controllo. Include le seguenti informazioni:

- 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 (AWS CLI)

1. Per identificare il controllo che desideri esaminare, esegui il comando [Elenco-controlli](#) e specifica un `--control-type`. In entrambi i casi, è possibile recuperare un elenco di controlli standard. In alternativa, puoi recuperare un elenco di controlli personalizzati.

Nell'esempio seguente, sostituisci il *testo segnaposto* con Customo Standard.

```
aws auditmanager list-controls --control-type Custom/Standard
```

La risposta restituisce un elenco di controlli. Trova il controllo che desideri verificare e prendi nota dell'ID di controllo e del nome della risorsa Amazon (ARN).

2. Per ottenere i dettagli di controllo, esegui il comando [get-control](#) e specifica `--control-id`.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

I dettagli di controllo vengono restituiti in formato JSON. Per comprendere questi dati, consulta [get-control Output](#) nel AWS CLI Riferimento ai comandi.

3. Per visualizzare i tag di un controllo, usa il [list-tags-for-resource](#) comando e specifica il `--resource-arn` per il controllo.

Nell'esempio seguente, sostituisci il *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
```

Per ulteriori informazioni sul tagging in Audit Manager, consulta [Tagging delle risorse AWS Audit Manager](#).

Audit Manager API

Per visualizzare i dettagli di controllo (API)

1. Per identificare il controllo da esaminare, utilizzate l'[ListControls](#) operazione e specificate un [ControlType](#). In entrambi i casi, puoi restituire un elenco di controlli standard. In alternativa, puoi restituire un elenco di controlli personalizzati.

Dalla risposta, trova il controllo che si desidera esaminare e prendi nota dell'ID del controllo e del relativo nome della risorsa Amazon (ARN).

2. Per ottenere i dettagli del controllo, utilizzate l'[GetControl](#) operazione. Nella richiesta, specifica l'[controlId](#) ottenuto dalla fase 1.

I dettagli di controllo vengono restituiti in formato JSON. Per comprendere questi dati, consulta [GetControl Response Elements](#) nell'AWS Audit Manager API Reference.

3. Per vedere i tag per il controllo, usa l'[ListTagsForResource](#) operazione. Nella richiesta, specifica il controllo [resourceArn](#) dalla fase 1.

Per ulteriori informazioni sul tagging in Audit Manager, consulta [Tagging delle risorse AWS Audit Manager](#).

Per ulteriori informazioni su queste operazioni API, scegli i link precedenti per leggere la AWS Audit Manager Documentazione di riferimento dell'API. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Creazione di un controllo personalizzato

Puoi utilizzare controlli personalizzati per raccogliere prove da fonti di dati specifiche da te definite.

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:

Usa un controllo esistente come punto di partenza

È possibile personalizzare qualsiasi controllo in Audit Manager. Questa è una buona opzione se un controllo esistente soddisfa più o meno il vostro obiettivo, ma desiderate estenderne le linee guida o modificare alcuni attributi per soddisfare le vostre esigenze specifiche. Ad esempio, è possibile modificare la frequenza con cui un controllo raccoglie le prove e quindi modificare il nome del controllo.

Crea un controllo personalizzato per gli audit interni

Per supportare gli audit interni, puoi creare un controllo personalizzato appositamente progettato che non sia correlato a nessun framework o regolamento di conformità specifico. In questo modo hai la libertà di adattare i requisiti di controllo a una particolare area o raccogliere prove da una risorsa specifica dell'attività. Ad esempio, puoi creare un controllo personalizzato che utilizza le AWS Config regole personalizzate della tua organizzazione come fonte di dati per la raccolta di prove.

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. In questo caso, il nome del controllo può essere una domanda e puoi fornire una risposta caricando un file o inserendo una risposta testuale come prova manuale.

Esistono due modi per creare un controllo personalizzato. È possibile creare un nuovo controllo partendo da zero oppure personalizzare un controllo esistente.

Argomenti

- [Creare un nuovo controllo personalizzato da zero](#)
- [Personalizzazione di un controllo esistente](#)

Creare un nuovo controllo personalizzato da zero

Puoi creare un nuovo controllo personalizzato partendo da zero seguendo queste fasi.

Important

Consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi a formato libero come Dettagli di controllo, Informazioni sui test o Piano di azione. Se crei controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Argomenti

- [Fase 1: specifica dei dettagli di controllo](#)
- [Fase 2: impostazione delle origini dati](#)
- [Fase 3 \(Facoltativo\): Definizione di un piano di azione](#)
- [Fase 4: Revisione e creazione del controllo](#)
- [Cosa posso fare dopo?](#)

Fase 1: specifica dei dettagli di controllo

Inizia specificando i dettagli di controllo personalizzato.

Per specificare i dettagli di controllo

1. Apri la console 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: impostazione delle origini dati

Successivamente, definisci fino a 10 fonti di dati. Un'origine dati determina da dove il controllo personalizzato raccoglie le prove.

Se desideri raccogliere prove automatizzate, ogni fonte di dati deve includere 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 invece desideri fornire le tue prove, assegnerai un nome alla fonte dei dati e poi sceglierai un'opzione di prova manuale.

Important

Per utilizzare correttamente AWS Config e Security Hub come fonti di dati automatizzate, assicurati di fare quanto segue:

- Segui le istruzioni per [configurare AWS Config](#) e [configurare Security Hub](#) da utilizzare con Audit Manager.
- Includi entrambi AWS Config e Security Hub come servizi inclusi nella valutazione.

Audit Manager può quindi raccogliere prove ogni volta che viene effettuata una valutazione delle AWS Config regole o dei controlli del Security Hub specificati in questo passaggio.

Configurazione delle origini dati

1. In Nome origine dati, sostituisci il testo segnaposto con un nome descrittivo per l'origine dati.
2. In Metodo di raccolta delle prove, scegli come raccogliere le prove per questo controllo.
 - a. Se desideri che Audit Manager raccolga prove, scegli Automatizzato e segui queste fasi:
 - In Tipo di origine dati, specifica da dove Audit Manager raccoglie le prove automatiche.

- Per AWS CloudTrail, scegli una parola chiave per il nome dell'evento dall'elenco a discesa.
- Ad esempio AWS Config, seleziona un tipo di regola e quindi scegli una parola chiave che identifichi la regola dall'elenco a discesa.
- Per AWS Security Hub, scegli un controllo Security Hub dall'elenco a discesa.
- Per le AWS chiamate API, scegli una chiamata API, quindi seleziona una frequenza di raccolta delle prove.

 Tip

Per una panoramica di ogni tipo di origine dati e dei relativi suggerimenti per la risoluzione dei problemi, consulta [Panoramica delle fonti di dati automatizzate](#). Se devi convalidare la configurazione della tua origine dati con un esperto di dominio, imposta per adesso il metodo di raccolta delle prove su Manuale. In tal modo, puoi creare il controllo e aggiungerlo subito a un framework, quindi [modificarlo in base alle esigenze](#) in un secondo momento.

- b. Se desideri fornire le tue prove, scegli Manuale e seleziona un'opzione Prova manuale.
 - Caricamento del file: seleziona questa opzione se il controllo richiede la documentazione come prova.
 - Risposta testuale: selezionare questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.
3. (Facoltativo) In Dettagli aggiuntivi, inserisci una descrizione dell'origine dati e una descrizione della risoluzione dei problemi.
4. (Facoltativo) Per aggiungere un'altra origine, scegliere Aggiungi origine dati, quindi ripeti i passaggi 1-3.
5. (Facoltativo) Per rimuovere un'origine dati, scegli Rimuovi nella parte superiore della casella di configurazione dell'origine dati.
6. Quando hai terminato, seleziona Successivo.

Fase 3 (Facoltativo): Definizione di un piano di azione

Successivamente, specifica le azioni da intraprendere se è necessario correggere questo controllo.

Per definire un piano di azione

1. In Titolo, inserisci un titolo descrittivo per il piano di azione.
2. In Istruzioni per il piano di azione, inserisci istruzioni dettagliate per il piano di 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.

Cosa posso fare dopo?

Dopo aver creato un nuovo controllo personalizzato, puoi aggiungerlo a un framework personalizzato. Per ulteriori informazioni, consulta [Creazione di un framework personalizzato](#) e [Modifica di un framework personalizzato](#).

Dopo aver aggiunto il controllo personalizzato a un framework personalizzato, puoi creare una valutazione da tale framework personalizzato e iniziare a raccogliere prove. Per ulteriori informazioni, consulta [Creazione di una valutazione](#).

Per suggerimenti sulla risoluzione dei problemi, consulta [Risoluzione dei problemi relativi ai controlli e ai set di controlli](#).

Personalizzazione di un controllo esistente

Invece di creare un controllo personalizzato da zero, puoi utilizzare un controllo esistente come punto di partenza e personalizzarlo in base alle tue esigenze. Quando esegui questa operazione, il controllo esistente rimane nella libreria di controllo e viene creato un nuovo controllo personalizzato con le impostazioni personalizzate.

È possibile selezionare qualsiasi controllo esistente da personalizzare. Può essere un controllo standard o personalizzato.

Important

Consigliamo vivamente di non inserire mai informazioni identificative sensibili in campi a formato libero come Dettagli di controllo, Informazioni sui test o Piano di azione. Se crei

controlli personalizzati che contengono informazioni sensibili, non puoi condividere nessuno dei tuoi framework personalizzati che contengono questi controlli.

Argomenti

- [Fase 1: specifica dei dettagli di controllo](#)
- [Fase 2: impostazione delle origini dati](#)
- [Fase 3: \(facoltativa\): Definizione di un piano di azione](#)
- [Fase 4: Revisione e creazione del controllo](#)
- [Cosa posso fare dopo?](#)

Fase 1: specifica dei dettagli di controllo

I dettagli di controllo vengono ereditati dal controllo originale. Esamina e modifica di questi dettagli in base alle esigenze.

Per specificare i dettagli di controllo

1. Apri la console 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 che desideri personalizzare, quindi scegli Personalizza il controllo esistente.
4. Specifica il nuovo nome del controllo e scegli Personalizza.
5. In Dettagli di controllo, personalizza i dettagli di controllo in base alle esigenze.
6. In Informazioni sui test, personalizza le informazioni sui test in base alle esigenze.
7. In Tag, personalizza i tag in base alle esigenze.
8. Seleziona Successivo.

Fase 2: impostazione delle origini dati

Le origini dei dati vengono ereditate dal controllo originale. Puoi modificare, aggiungere o rimuovere le fonti di dati in base alle esigenze.

⚠ Important

Per utilizzare correttamente AWS Config e Security Hub come fonti di dati automatizzate, assicurati di fare quanto segue:

- Segui le istruzioni per [configurare AWS Config](#) [configurare Security Hub](#) da utilizzare con Audit Manager.
- Includi entrambi AWS Config e Security Hub come servizi inclusi nella valutazione.

Audit Manager può quindi raccogliere prove ogni volta che viene effettuata una valutazione delle AWS Config regole o dei controlli del Security Hub specificati in questo passaggio.

Configurazione delle origini dati

1. In Nome origine dati, personalizza il nome dell'origine dati in base alle esigenze.
2. In Metodo di raccolta delle prove, personalizza la selezione in base alle esigenze.
 - a. Se desideri che Audit Manager raccolga prove, scegli Automatizzato e segui queste fasi:
 - In Tipo di origine dati, esamina da dove Audit Manager raccoglie le prove automatiche e modifica in base alle necessità.
 - Per AWS CloudTrail, scegli una parola chiave per il nome dell'evento dall'elenco a discesa.
 - Ad esempio AWS Config, seleziona un tipo di regola e quindi scegli una parola chiave che identifichi la regola dall'elenco a discesa.
 - Per AWS Security Hub, scegli un controllo Security Hub dall'elenco a discesa.
 - Per le AWS chiamate API, scegli una chiamata API, quindi seleziona una frequenza di raccolta delle prove.

ℹ Tip

Per una panoramica di ogni tipo di origine dati e dei relativi suggerimenti per la risoluzione dei problemi, consulta [Panoramica delle fonti di dati automatizzate](#). Se devi convalidare la configurazione della tua origine dati con un esperto di dominio, imposta per adesso il metodo di raccolta delle prove su Manuale. In

tal modo, puoi creare il controllo e aggiungerlo subito a un framework, quindi [modificarlo in base alle esigenze](#) in un secondo momento.

- b. Se desideri fornire le tue prove, scegli Manuale e seleziona un'opzione Prova manuale.
 - Caricamento del file: seleziona questa opzione se il controllo richiede la documentazione come prova.
 - Risposta testuale: selezionare questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.
3. (Facoltativo) In Dettagli aggiuntivi, apporta le modifiche necessarie alla descrizione dell'origine dati o alla descrizione della risoluzione dei problemi.
4. (Facoltativo) Per aggiungere un'altra origine, scegli Aggiungi origine dati.
5. (Facoltativo) Per rimuovere un'origine dati, scegli Rimuovi.
6. 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.

Per definire un piano di azione

1. In Titolo, rivedi il titolo del piano di azione e personalizzalo in base alle esigenze.
2. In Istruzioni per il piano di azione, rivedi e personalizza le istruzioni in base alle esigenze.
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.

Cosa posso fare dopo?

Dopo aver creato un nuovo controllo personalizzato, puoi aggiungerlo a un framework personalizzato. Per ulteriori informazioni, consulta [Creazione di un framework personalizzato](#) e [Modifica di un framework personalizzato](#).

Dopo aver aggiunto un controllo personalizzato a un framework personalizzato, puoi creare una valutazione da tale framework personalizzato e iniziare a raccogliere prove. Per ulteriori informazioni, consulta [Creazione di una valutazione](#).

Se devi modificare un controllo personalizzato, consulta [Modifica di un controllo personalizzato](#).

Per suggerimenti sulla risoluzione dei problemi, consulta [Risoluzione dei problemi relativi ai controlli e ai set di controlli](#).

Modifica di un controllo personalizzato

Puoi modificare un controllo personalizzato in Audit Manager seguendo queste fasi.

Argomenti

- [Fase 1: modifica dei dettagli di controllo](#)
- [Fase 2: modifica origini dati](#)
- [Fase 3: modifica di un piano di azione \(facoltativo\)](#)
- [Fase 4: Revisione e aggiornamento del controllo](#)

Fase 1: modifica dei dettagli di controllo

Inizia esaminando e modificando i dettagli di controllo secondo necessità.

Per modificare i dettagli di controllo

1. Apri la console 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 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 le informazioni sui test consigliati in base alle esigenze.
6. Seleziona Successivo.

i Tip

Per modificare i tag di un controllo, apri il controllo e scegli la [scheda dei tag](#). Qui puoi visualizzare e modificare i tag associati al controllo.

Fase 2: modifica origini dati

Successivamente, puoi modificare, rimuovi o aggiungi origini dati per il controllo.

⚠ Important

Per utilizzare correttamente AWS Config e Security Hub come fonti di dati automatizzate, assicurati di fare quanto segue:

- Segui le istruzioni per [configurare AWS Config](#) [configurare Security Hub](#) da utilizzare con Audit Manager.
- Includi entrambi AWS Config e Security Hub come servizi inclusi nella valutazione.

Audit Manager può quindi raccogliere prove ogni volta che viene effettuata una valutazione delle AWS Config regole o dei controlli del Security Hub specificati in questo passaggio.

Per modificare le origini dati

1. In Nome dell'origine dati, rivedi il nome corrente e modificalo secondo necessità.
2. In Metodo di raccolta delle prove, esamina la selezione corrente e modifica in base alle necessità.
 - a. Se desideri che Audit Manager raccolga prove, scegli Automatizzato e segui queste fasi:
 - In Tipo di origine dati, esamina da dove Audit Manager raccoglie le prove automatiche e modifica in base alle necessità.
 - Per AWS CloudTrail, scegli una parola chiave per il nome dell'evento dall'elenco a discesa.
 - Ad esempio AWS Config, seleziona un tipo di regola e quindi scegli una parola chiave che identifichi la regola dall'elenco a discesa.

- Per AWS Security Hub, scegli un controllo Security Hub dall'elenco a discesa.
- Per le AWS chiamate API, scegli una chiamata API, quindi seleziona una frequenza di raccolta delle prove.

 Tip

Per una panoramica di ogni tipo di origine dati e dei relativi suggerimenti per la risoluzione dei problemi, consulta [Panoramica delle fonti di dati automatizzate](#).

- b. Se desideri fornire le tue prove, scegli Manuale e seleziona un'opzione Prova manuale.
 - Caricamento del file: seleziona questa opzione se il controllo richiede la documentazione come prova.
 - Risposta testuale: selezionare questa opzione se il controllo richiede una risposta a una domanda di valutazione del rischio.
3. (Facoltativo) In Dettagli aggiuntivi, apporta le modifiche necessarie alla descrizione dell'origine dati o alla descrizione della risoluzione dei problemi.
4. (Facoltativo) Per aggiungere un'altra origine, scegli Aggiungi origine dati.
5. (Facoltativo) Per rimuovere un'origine dati, scegli Rimuovi.
6. Seleziona Successivo.

Fase 3: modifica di un piano di azione (facoltativo)

Successivamente, rivedi e modifica il piano di azione facoltativo.

Per modificare un piano di azione

1. In Titolo, modifica il titolo in base alle esigenze.
2. In Istruzioni per il piano di azione, modifica le istruzioni in base alle esigenze.
3. Seleziona Successivo.

Fase 4: Revisione e aggiornamento del controllo

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.

Eliminazione di un controllo personalizzato

È possibile utilizzare la libreria di controllo per eliminare un controllo personalizzato indesiderato. Dopo aver eliminato un controllo, questo non viene più visualizzato nella libreria di controllo. Puoi anche eliminare i controlli personalizzati utilizzando 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, Audit Manager 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 (console)

1. Apri la console 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 (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 il *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 (API)

1. Utilizzate l'[ListControls](#) operazione e specificate [ControlType](#) come Custom. Dalla risposta, individua il controllo che desideri eliminare e annota l'ID del controllo.
2. Utilizzare l'[DeleteControl](#) operazione 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, scegli uno dei link precedenti per saperne di più nel [AWS Audit Manager Riferimento API](#). Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK specifici della lingua AWS .

Modifica della frequenza di raccolta delle prove per un controllo

AWS Audit Manager raccoglie prove da più fonti di dati con frequenze diverse. La frequenza di raccolta delle prove supportate dipende dal tipo di prove raccolte per il controllo.

- Per le chiamate API AWS , Audit Manager raccoglie prove utilizzando una chiamata API di descrizione a un'altra Servizio AWS. È possibile specificare la frequenza di raccolta delle prove direttamente in Audit Manager (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 regola AWS Config .
- Per AWS Security Hub, Audit Manager 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.

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

- [Istantanee di configurazione dalle chiamate API AWS](#)
- [Controlli di conformità da AWS Config](#)
- [Controlli di conformità da Security Hub](#)
- [Registri delle attività degli utenti da AWS CloudTrail](#)

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 che utilizza le chiamate API come origine dati.

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 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 personalizzato che desideri modificare e scegli Modifica.
4. Nella pagina Modifica dettagli controllo, scegli Avanti.
5. Individua la casella dell'origine dati che desideri modificare e verifica che le seguenti informazioni siano corrette:
 - Il metodo di raccolta delle prove è automatizzato.
 - Il tipo di origine dati sono le chiamate API AWS .
 - La chiamata API selezionata è quella di cui si desidera modificare la frequenza.
6. In Frequenza, scegli la frequenza con cui desideri raccogliere le prove per il controllo personalizzato.
7. Ripeti le fasi 5-6, se necessario, per tutte le fonti di dati di chiamata API aggiuntive che desideri modificare.
8. Seleziona Successivo.
9. Nella pagina Modifica un piano di azione, scegli Avanti.
10. Nella pagina Rivedi e aggiorna il controllo, esamina le informazioni relative al controllo personalizzato. Per modificare le informazioni relative a una fase, scegli Modifica.
11. Al termine, scegli Salva le modifiche.

Dopo aver modificato un controllo con chiamate API AWS come tipo di origine dati, 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 Audit Manager. 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.

Fonti di dati di controllo supportate 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

I seguenti argomenti riassumono ciascuno di questi tipi di origini dati automatizzate ed elencano AWS Security Hub i controlli, AWS Config le regole e le chiamate AWS API specifici supportati da Audit Manager.

Argomenti

- [Panoramica delle fonti di dati automatizzate](#)
- [Regole di AWS Config supportato da AWS Audit Manager](#)
- [AWS Security Hub controlli supportati da AWS Audit Manager](#)
- [Chiamate API supportate da AWS Audit Manager](#)
- [AWS CloudTrail nomi di eventi supportati da AWS Audit Manager](#)

Panoramica delle fonti di dati automatizzate

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 delle attività di un utente specifico.	Continuo.	Seleziona dall'elenco dei nomi di eventi supportati .	Audit Manager filtra CloudTrail i log in base alla parola chiave scelta. I risultati vengono importati come prove dell'attività dell'utente.	La mia valutazione non sta raccogliendo prove dell'attività degli utenti da AWS CloudTrail!
AWS Config	Acquisisce un'istantanea del vostro stato di sicurezza	In base ai trigger definiti nella regola. AWS Config	Scegli una regola, quindi seleziona una regola. <ul style="list-style-type: none"> Per le regole gestite, seleziona dall'elenco delle parole chiave 	Audit Manager ottiene i risultati di questa regola direttamente da AWS Config. Il risultato viene importato come	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
	delle risorse riportando i risultati di. AWS Config		<p>supportate per le regole gestite.</p> <ul style="list-style-type: none"> Per le regole personalizzate, seleziona dall'elenco delle regole disponibili. 	prova del controllo di conformità.	<p>raccolgendo prove di verifica della conformità a da AWS Config AWS Config problemi di integrazione</p>

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 del livello di sicurezza delle risorse riportando i risultati Security Hub.	In base alla pianificazione del controllo Security Hub.	Seleziona dall'elenco degli ID di controllo Security Hub supportati .	Audit Manager 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 chiama API	Scatta un'istanza 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.	Audit Manager 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

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.

Note

- Audit Manager 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. Per ulteriori informazioni, consulta la sezione di [Risoluzione dei problemi](#) di questa guida.
- 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 Config](#) affinché 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 [1.9. Assicurarsi che i criteri delle password IAM richiedano una lunghezza minima di 14 o superiore](#). In AWS Config, la [iam-password-policy](#) regola 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](#).

Argomenti

- [Utilizzo di regole AWS Config gestite con Audit Manager](#)
- [Utilizzo di regole AWS Config personalizzate con Audit Manager](#)
- [Risoluzione dei problemi di AWS Config integrazione con Audit Manager](#)

Utilizzo di regole AWS Config gestite con Audit Manager

326 regole AWS Config gestite sono attualmente 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 Audit Manager 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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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](#)

Parole chiave AWS Config gestite supportate

- [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](#)
- [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 ora 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.

Per istruzioni su come creare un controllo che utilizza regole personalizzate come origine dati, consulta [Creazione di un nuovo controllo da zero](#) e [Personalizzazione di un controllo esistente](#).

Tip

Tieni presente che le regole gestite non vengono visualizzate nell'elenco a discesa delle regole personalizzate in Audit Manager.

Se desideri 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.

	Name	Remediation action	Type	Compliance
<input type="radio"/>	account-part-of-organizations	Not set	AWS managed	 Compliant

Per mappare una regola gestita come origine dati, puoi cercare la parola chiave Identificatore Regola Gestita in Audit Manager nell'elenco a discesa delle regole gestite. Per ulteriori informazioni, consulta la sezione di [Risoluzione dei problemi](#) di questa guida.

Dopo aver mappato le regole personalizzate come origine dati per un controllo, puoi associare tale controllo a un framework personalizzato in Audit Manager. Per istruzioni su come creare un framework personalizzato che utilizza il controllo personalizzato, consulta [Creazione di un nuovo framework da zero](#) e [Personalizzazione di un framework esistente](#). Per istruzioni su come aggiungere il controllo a un framework personalizzato esistente, consulta [Modifica di un framework esistente](#).

Per informazioni sulla creazione di una regola personalizzata in AWS Config, consulta [Sviluppo di una regola personalizzata AWS Config nella Guida per gli AWS Config sviluppatori](#).

Risoluzione dei problemi di AWS Config integrazione con Audit Manager

Per trovare risposte a domande e problemi comuni, consulta [integrazione AWS Config](#) nella sezione Risoluzione dei problemi di questa guida.

AWS Security Hub controlli supportati da AWS Audit Manager

Audit Manager consente di riportare i risultati dei controlli di conformità direttamente da Security Hub. A tale scopo, specifica uno o più controlli Security Hub come mappatura dell'origine dati quando configuri un controllo personalizzato in Audit Manager.

Note

- Audit Manager non raccoglie prove dalle [AWS Config regole collegate ai servizi create da Security Hub](#). Per ulteriori informazioni, consulta la sezione di [Risoluzione dei problemi](#) di questa guida.
- 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](#).

Argomenti

- [Utilizzo dei controlli Security Hub con Audit Manager](#)
- [Controlli Security Hub supportati](#)

Utilizzo dei controlli Security Hub con Audit Manager

Tip

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 2023, 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 Audit Manager. Di conseguenza, i risultati consolidati comportano una diminuzione delle valutazioni totali delle risorse uniche eseguite da Audit Manager per i risultati Security Hub. Per tale motivo, l'utilizzo di risultati consolidati può spesso portare a una riduzione dei costi di utilizzo dell'Audit Manager, 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 Audit Manager 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 del controllo consolidato è attivata, Security Hub genera un singolo risultato per questo controllo.
- Security Hub invia i risultati consolidati all'Audit Manager per questo controllo.
- Il risultato consolidato conta come un'unica valutazione delle risorse in Audit Manager. 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 all'Audit Manager per questo controllo.
- Il conteggio dei tre risultati come un'unica valutazione delle tre risorse in Audit Manager. 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 Audit Manager (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 Audit Manager. 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 Audit Manager (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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	1.20	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.
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	3.7	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
PCI DSS	FOTO. AutoScaling1.	AutoScaling.1.
PCI DSS	PCI. CloudTrai I1.	CloudTrail.1.
PCI DSS	PCI. CloudTrai I2.	CloudTrail2.
PCI DSS	PCI. CloudTrai I3.	CloudTrail3.

Standard di sicurezza	Parola chiave supportata in Audit Manager (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (ID di controllo standard nel Security Hub)	Documentazione di controllo correlata (ID di controllo di sicurezza corrispondente nel Security Hub)
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
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 Migliori pratiche di sicurezza di base	Account.2	Conto.2
AWS Migliori pratiche di sicurezza di base	ACM.1	ACM.1

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	ACM.2	ACM.2
AWS Migliori pratiche di sicurezza di base	APIGateway.1	APIGateway.1
AWS Migliori pratiche di sicurezza di base	APIGateway.2	APIGateway.2
AWS Migliori pratiche di sicurezza di base	APIGateway.3	APIGateway.3
AWS Migliori pratiche di sicurezza di base	APIGateway.4	APIGateway.4
AWS Migliori pratiche di sicurezza di base	APIGateway.5	APIGateway.5
AWS Migliori pratiche di sicurezza di base	APIGateway.8	APIGateway.8
AWS Migliori pratiche di sicurezza di base	APIGateway.9	APIGateway.9
AWS Migliori pratiche di sicurezza di base	AppSync2.	AppSync2.
AWS Migliori pratiche di sicurezza di base	AppSync5.	AppSync5.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	Atena.1	Atena.1
AWS 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
AWS 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 Best practice di sicurezza di base	CloudFormation1.	CloudFormation.1.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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.
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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.
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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.
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	CodeBuild5.	CodeBuild5.
AWS Migliori pratiche di sicurezza di base	Config.1	Config.1
AWS Migliori pratiche di sicurezza di base	DMS.1	DMS.1
AWS Migliori pratiche di sicurezza di base	DMS.6	DMS.6
AWS Migliori pratiche di sicurezza di base	DMS.7	DMS.7
AWS Migliori pratiche di sicurezza di base	DMS.8	DMS.8
AWS Migliori pratiche di sicurezza di base	DMS.9	DMS.9
AWS Migliori pratiche di sicurezza di base	Documento DB.1	Documento DB.1
AWS Migliori pratiche di sicurezza di base	Documento DB.2	Documento DB.2
AWS Migliori pratiche di sicurezza di base	Documento DB.3	Documento DB.3

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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 Migliori pratiche di sicurezza di base	DynamoDB.2	DynamoDB.2
AWS Migliori pratiche di sicurezza di base	DynamoDB.3	DynamoDB.3
AWS Migliori pratiche di sicurezza di base	Dynamo DB.4	Dynamo DB.4
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 Migliori pratiche di sicurezza di base	EC2.2	EC2.2
AWS Migliori pratiche di sicurezza di base	EC2.3	EC2.3

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	EC2.4	EC2.4
AWS Migliori pratiche di sicurezza di base	EC2.6	EC2.6
AWS Migliori pratiche di sicurezza di base	EC2.7	EC2.7
AWS Migliori pratiche di sicurezza di base	EC2.8	EC2.8
AWS Migliori pratiche di sicurezza di base	EC2.9	EC2.9
AWS Migliori pratiche di sicurezza di base	EC2.10	EC2.10
AWS Migliori pratiche di sicurezza di base	EC2.12	EC2.12
AWS Migliori pratiche di sicurezza di base	EC2.13	EC2.13
AWS Migliori pratiche di sicurezza di base	EC 2.14	EC 2.14
AWS Migliori pratiche di sicurezza di base	EC2.15	EC2.15

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	EC2.16	EC2.16
AWS Migliori pratiche di sicurezza di base	EC2.17	EC2.17
AWS Migliori pratiche di sicurezza di base	EC2.18	EC2.18
AWS Migliori pratiche di sicurezza di base	EC2.19	EC2.19
AWS Migliori pratiche di sicurezza di base	EC2.20	EC2.20
AWS Migliori pratiche di sicurezza di base	EC2.21	EC2.21
AWS Migliori pratiche di sicurezza di base	EC2.22	EC2.22
AWS Migliori pratiche di sicurezza di base	EC2.23	EC2.23
AWS Migliori pratiche di sicurezza di base	EC2.24	EC2.24
AWS Migliori pratiche di sicurezza di base	EC2.25	EC2.25

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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 Migliori pratiche di sicurezza di base	ECR.2	ECR.2
AWS Migliori pratiche di sicurezza di base	ECR.3	ECR.3
AWS Migliori pratiche di sicurezza di base	ECS.1	ECS.1
AWS Migliori pratiche di sicurezza di base	ECS.2	ECS.2
AWS Migliori pratiche di sicurezza di base	ECS.3	ECS.3
AWS Migliori pratiche di sicurezza di base	ECS.4	ECS.4
AWS Migliori pratiche di sicurezza di base	ECS.5	ECS.5

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	ECS.8	ECS.8
AWS Migliori pratiche di sicurezza di base	ECS.9	ECS.9
AWS Migliori pratiche di sicurezza di base	ECS.10	ECS.10
AWS Migliori pratiche di sicurezza di base	ECS.12	ECS.12
AWS Migliori pratiche di sicurezza di base	EFS.1	EFS.1
AWS Migliori pratiche di sicurezza di base	EFS.2	EFS.2
AWS Migliori pratiche di sicurezza di base	EFS.3	EFS.3
AWS Migliori pratiche di sicurezza di base	EFS.4	EFS.4
AWS Migliori pratiche di sicurezza di base	EKS.1	EKS.1
AWS Migliori pratiche di sicurezza di base	EKS.2	EKS.2

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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.
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Migliori pratiche di sicurezza di base	ELB.1	ELB.1
AWS Migliori pratiche di sicurezza di base	ELB.2	ELB.2
AWS Migliori pratiche di sicurezza di base	ELB.3	ELB.3
AWS Migliori pratiche di sicurezza di base	ELB.4	ELB.4
AWS Migliori pratiche di sicurezza di base	ELB.5	ELB.5
AWS 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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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 Migliori pratiche di sicurezza di base	GuardDuty1.	GuardDuty.1.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	SONO 22	IO SONO 22
AWS 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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	Macie.1	Macie.1
AWS 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 Migliori pratiche di sicurezza di base	MSK.2	MSK.2
AWS Migliori pratiche di sicurezza di base	Nettuno.1	Nettuno.1
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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.
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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
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 Migliori pratiche di sicurezza di base	S3.1	S3.1
AWS Migliori pratiche di sicurezza di base	S3.2	S3.2

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	S3.3	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
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

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	S3.14	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.
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	SecretsMa nager1.	SecretsManager.1.
AWS Migliori pratiche di sicurezza di base	SecretsMa nager2.	SecretsManager2.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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	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
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.

Standard di sicurezza	Parola chiave supportata in Audit Manager (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.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
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 Migliori pratiche di sicurezza di base	WAF.12	WAF.12

Chiamate API supportate da AWS Audit Manager

Audit Manager effettua chiamate API Servizi AWS per raccogliere un'istantanea dei dettagli di configurazione AWS delle risorse. Puoi specificare queste chiamate API come mappatura dell'origine dati quando configuri un controllo personalizzato in Audit Manager.

Per ogni risorsa che rientra nell'ambito di una chiamata API, Audit Manager 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.

In questa pagina

- [Chiamate API supportate per fonti di dati di controllo personalizzate](#)
- [Chiamate API impaginate](#)
- [Chiamate API utilizzate nel framework standard AWS License Manager](#)

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 utilizzato 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.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
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 chiamate dei modelli nel tuo Account AWS
cloudfront_ListDistributions	Recupera un elenco di tutte le distribuzioni presenti nel tuo Account AWS
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_DescribeConfigRules	Recupera i dettagli sulle tue AWS Config regole.
config_DescribeDeliveryChannels	Raccogli uno snapshot di configurazione per i canali di distribuzione nel tuo Account AWS.
connessione_diretta_DescribeDirectConnectGateways	Recupera un elenco di tutti i tuoi gateway. AWS Direct Connect
directconnect_DescribeVirtualGateways	Recupera un elenco dei gateway virtuali privati di proprietà del tuo Account AWS.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
docdb_DescribeCertificates	Raccogli un elenco di certificati per il tuo Account AWS.
docdb_describeDBClusterParameterGroups	Raccogli un elenco di descrizioni <code>DBClusterParameterGroup</code> per il tuo Account AWS.
docdb_DescribeDBInstances	Raccogli informazioni sulle istanze Amazon DynamoDB con provisioning nel tuo Account AWS.
dynamodb_DescribeTable	<p>Raccogli snapshot di configurazione per le tabelle DynamoDB nel tuo Account AWS.</p> <p>Quando utilizzi questa API come origine dati, non è necessario fornisci il nome di una tabella DynamoDB specifica. Al contrario, Audit Manager utilizza l'operazione <code>ListTables</code> per elencare tutte le tabelle. Per ogni tabella elencata, Audit Manager esegue quindi l'operazione <code>DescribeTable</code> per generare prove per quella risorsa.</p>
dynamodb_ListBackups	Recupera un elenco dei backup DynamoDB associati al tuo Account AWS.
dynamodb_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.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
ec2_DescribeFlowLogs	Raccogli uno snapshot dei log di flusso.
ec2_DescribeInstances	Raccogli uno snapshot delle istanze.
ec2_DescribeInternetGateways	Raccogli uno snapshot dei gateway Internet.
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.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
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.
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.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
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.
elasticache_DescribeServiceUpdates	Raccogli un'istantanea degli aggiornamenti del servizio per Amazon ElastiCache.
elasticfilesystem_DescribeAccessPoints	Raccogli un'istantanea dei punti di accesso Amazon EFS nel tuo Account AWS.
elasticfilesystem_DescribeFileSystems	Raccogli uno snapshot dei tuoi file system Amazon EFS.
bilanciamento del carico elastico v2_DescribeLoadBalancers	Raccogli un'istantanea dei sistemi di bilanciamento del carico del tuo Account AWS
elasticloadbalancingv2_DescribeSSLPolicies	Raccogli uno snapshot delle policy utilizzate per la negoziazione SSL.
elasticloadbalancingv2_DescribeTargetGroups	Raccogli uno snapshot dei tuoi gruppi target ELB.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
elasticmap_reduce_ListSecurityConfigurations	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_ListConnessioni	Recupera un elenco delle EventBridge connessioni Amazon nel tuo Account AWS.
eventi_ListEventBuses	Recupera un elenco dei bus di EventBridge eventi Amazon presenti nel tuo sito Account AWS, inclusi il bus eventi predefinito, gli event bus personalizzati e gli event bus dei partner.
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 <code>detectorIds</code> 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.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
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
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_ListKafkaVersions	Recupera un elenco degli oggetti versione di Apache Kafka nel tuo Account AWS.
cinesi_ListStreams	Recupera un elenco dei tuoi flussi di dati Kinesis.

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
km_GetKeyPolicy	<p>Gestione audit utilizza questa API per raccogliere uno snapshot delle policy della chiave per le AWS KMS keys nel tuo Account AWS.</p> <p>Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di una specifica AWS KMS key. Al contrario, Audit Manager utilizza l'operazione <code>ListKeys</code> per elencare tutte le chiavi KMS. Per ogni chiave KMS elencata, Audit Manager esegue quindi l'operazione <code>GetKeyPolicy</code> per generare prove per quella risorsa.</p>
kms_GetKeyRotationStatus	<p>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.</p> <p>Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di una specifica AWS KMS key. Al contrario, Audit Manager utilizza l'operazione <code>ListKeys</code> per elencare tutte le chiavi KMS. Per ogni chiave KMS elencata, Audit Manager esegue quindi l'operazione <code>GetKeyRotationStatus</code> per generare prove per quella risorsa.</p>
kms_ListKeys	<p>Recupera un elenco di quelli presenti nel AWS KMS keys tuo. Account AWS</p>
lambda_ListFunctions	<p>Recupera un elenco di funzioni Lambda nel Account AWS tuo, con la configurazione specifica della versione di ciascuna.</p>
rds_DescribeDBInstances	<p>Raccogli uno snapshot dei cluster Amazon Aurora DB e dei cluster DB Multi-AZ esistenti nel tuo. Account AWS</p>
rds_DescribeDBInstances	<p>Raccogli uno snapshot delle istanze RDS con provisioning nel tuo Account AWS.</p>
rds_DescribeDBInstanceAutomatedBackups	<p>Raccogli un'istantanea dei backup per le istanze correnti ed eliminate nel tuo. Account AWS</p>

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
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	<p>Raccogli uno snapshot che mostri la configurazione di crittografia predefinita per i tuoi bucket S3.</p> <p>Quando si utilizza questa API come fonte di dati, non è necessario fornire il nome di uno specifico bucket S3. Al contrario, Audit Manager utilizza l'operazione <code>ListBuckets</code> per elencare tutti i bucket. Per ogni bucket elencato, Audit Manager esegue quindi l'operazione <code>GetBucketEncryption</code> per generare prove per quella risorsa.</p> <p>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.</p>
s3_ListBuckets	Recupera un elenco dei bucket S3 presenti nel tuo. Account AWS
sagemaker_ListEndpointConfigs	Recupera un elenco delle configurazioni degli endpoint 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

Chiamata API supportata	In che modo Gestione audit utilizza questa API per raccogliere prove
waf-regional-ListRules	Recupera un elenco degli oggetti per il tuo. RuleSummary Account AWS
waf_ListRuleGroups	Recupera un elenco degli RuleGroupSummary oggetti per i gruppi di regole del tuo. Account AWS
waf_ListRules	Recupera un elenco degli RuleSummary oggetti per il tuo. Account AWS
waf_ListWebAcls	Recupera un elenco degli oggetti WebACLSummary per il tuo. Account AWS

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.

Alcune delle [chiamate API supportate da Audit Manager](#) sono impaginate. 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, Audit Manager 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, Audit Manager richiama l'operazione API impaginata più volte e ottiene ogni pagina di risultati fino alla restituzione di tutte le risorse. Per ogni risorsa, Audit Manager 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.

Audit Manager 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 utilizzate nel framework standard AWS License Manager

Nel framework standard [AWS License Manager](#), Audit Manager 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'[ListLicenseConfigurations](#) API, che fornisce dettagli sulle configurazioni delle licenze nell'account. Successivamente, aggiunge dati contestuali aggiuntivi per ogni configurazione di licenza [ListUsageForLicenseConfiguration](#) chiamando 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 and 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 CloudTrail nomi di eventi supportati da AWS Audit Manager

È possibile acquisire [gli eventi di AWS CloudTrail gestione e gli eventi di servizio globali](#) come prove in Audit Manager. A tale scopo, si specifica il nome dell' CloudTrail evento come parola chiave di mappatura dell'origine dati quando si crea un controllo personalizzato.

Note

Audit Manager 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 [GetObject](#) [ListBuckets](#) per 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 Audit Manager e dalle valutazioni e le prove per queste parole chiave non vengono più raccolte.

Impostazioni di AWS Audit Manager

Puoi rivedere e configurare le impostazioni AWS Audit Manager in qualsiasi momento.

Accesso alle impostazioni

1. Apri la console di Gestione audit AWS Audit all'[indirizzo https://console.aws.amazon.com/auditmanager/home](https://console.aws.amazon.com/auditmanager/home).
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.

Sono disponibili le impostazioni seguenti:

- [Impostazioni generali](#)
 - [Autorizzazioni](#)
 - [Crittografia dei dati](#)
 - [Amministratore delegato \(facoltativo\)](#)
 - [AWS Config \(facoltativo\)](#)
 - [Security Hub \(facoltativo\)](#)
 - [Disabilita AWS Audit Manager](#)
- [Impostazioni di valutazione](#)
 - [Proprietari di audit predefiniti \(opzionale\)](#)
 - [Destinazione del rapporto di valutazione \(opzionale\)](#)
 - [Notifiche \(facoltativo\)](#)
- [Impostazioni di evidence finder](#)
 - [Strumento evidence finder \(opzionale\)](#)
 - [Destinazione di esportazione \(facoltativo\)](#)

Impostazioni generali

La scheda Impostazioni generali è la visualizzazione predefinita della pagina delle impostazioni nella console Audit Manager. Utilizza questa scheda per rivedere e aggiornare le impostazioni generali di Audit Manager.

Argomenti

- [Autorizzazioni](#)
- [Crittografia dei dati](#)
- [Amministratore delegato \(facoltativo\)](#)
- [AWS Config \(facoltativo\)](#)
- [Security Hub \(facoltativo\)](#)
- [Disabilita AWS Audit Manager](#)

Autorizzazioni

AWS Audit Manager utilizza un ruolo collegato ai servizi per connettersi all'origine dati per conto dell'utente. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS Audit Manager](#).

Per esaminare i dettagli del ruolo collegato ai servizi utilizzato da Audit Manager, scegli Visualizza l'autorizzazione del ruolo collegato al servizio IAM.

Per ulteriori informazioni sui ruoli collegati al servizio, consulta [Utilizzo dei ruoli collegati al servizio](#) nella Guida per l'utente IAM.

Crittografia dei dati

Audit Manager crea automaticamente un'unica chiave gestita da AWS per l'archiviazione sicura dei dati. Per impostazione predefinita, i dati di Audit Manager sono crittografati con questa chiave KMS. In alternativa, 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.

Important

Per generare report di valutazione ed esportare correttamente i risultati della ricerca di evidence finder (individuazione delle prove), la chiave gestita dal cliente (se ne fornisci una) deve corrispondere alla stessa Regione AWS, come per la tua valutazione. Per un elenco delle Regioni Audit Manager, consulta la sezione [Endpoint e quote AWS Audit Manager](#) nei Riferimenti generali di Amazon Web Services.

È possibile aggiornare le impostazioni di crittografia dei dati utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI) o l'API Audit Manager.

Audit Manager console

Per aggiornare le impostazioni di crittografia dei dati (console)

1. Dalla scheda Impostazioni generali, vai alla sezione Crittografia dei dati.
2. Per utilizzare la chiave KMS predefinita fornita da Audit Manager, 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 (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 il *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 (API)

Esegui il comando [update-settings](#) e utilizza il parametro [kmsKey](#) per specificare la tua chiave gestita dal cliente.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWS specifici della lingua.

Note

Quando modifichi le impostazioni di crittografia dei dati di Audit Manager, 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. 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 istruzioni sulla creazione di chiavi, consulta [Creazione di chiavi](#) nella Guida per l'utente AWS Key Management Service.

Amministratore delegato (facoltativo)

Se utilizzi AWS Organization e desideri abilitare il supporto multi-account per Audit Manager, puoi designare un account membro della tua organizzazione come amministratore delegato per Audit Manager.

Prerequisiti

- L'account deve essere un membro di un'Organizzazione . Per ulteriori informazioni, consulta [Creazione e gestione di un'organizzazione](#) nella Guida per l'utente di AWS Organizations.
- 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, Audit Manager 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 Audit Manager. Per rivedere e modificare le impostazioni di crittografia, consulta [Crittografia dei dati](#).

Considerazioni importanti per gli amministratori delegati in Audit Manager

Prendi nota dei seguenti fattori che definiscono il modo in cui l'amministratore delegato opera in Audit Manager:

Gestione dell'utilizzo degli account

Non puoi utilizzare il tuo account di gestione AWS Organizations come amministratore delegato in Audit Manager.

Utilizzo di amministratori delegati su più utenti Regioni AWS

Se desideri abilitare Audit Manager in più di una regione Regione AWS, è necessario designare un account amministratore delegato separatamente in ciascuna regione. Nelle impostazioni di Audit Manager, è necessario utilizzare lo stesso account amministratore delegato in tutte le regioni.

Attività di pulizia di Evidence finder

Prima di utilizzare l'account di gestione per rimuovere o modificare un amministratore delegato, assicurati che l'account amministratore delegato corrente acceda a Audit Manager e disattivi lo strumento di evidence finder. Disabilitare evidence finder comporta l'eliminazione automatica di un archivio di dati degli eventi creato nell'account quando evidence finder era abilitato.

Se questa attività non viene completata, l'archivio di dati degli eventi rimane nel loro account. In questo caso, consigliamo all'amministratore delegato originale di utilizzare CloudTrail Lake per [eliminare manualmente l'archivio di 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, Audit Manager ignora un archivio di dati degli eventi non utilizzato. Tuttavia, se non elimini l'archivio di dati degli eventi inutilizzato, l'archivio continua a essere soggetto a costi di archiviazione CloudTrail Lake.

Eliminazione dei dati

Quando rimuovi 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 Audit Manager. In alternativa, puoi utilizzare una delle operazioni API di eliminazione fornite da Audit Manager. Per un elenco delle operazioni di eliminazione disponibili, vedere [Eliminazione dei dati di Audit Manager](#).

Al momento, Audit Manager non offre un'opzione per eliminare le prove per uno specifico amministratore delegato. Invece, quando il tuo account di gestione annulla la registrazione di Audit Manager, eseguiamo una pulizia dell'account amministratore delegato corrente al momento dell'annullamento della registrazione.

Per le soluzioni ai problemi più comuni relativi alle Organizzazioni e agli amministratori delegati in Audit Manager, consulta [Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations](#).

Gestione di un account amministratore delegato per Audit Manager

È possibile rivedere e modificare le impostazioni dell'account amministratore delegato come segue.

Per aggiungere un amministratore delegato

È possibile aggiungere un amministratore delegato utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI) o l'API Audit Manager.

Note

Dopo aver aggiunto un amministratore delegato nelle impostazioni di Audit Manager, l'account di gestione non può più creare valutazioni aggiuntive in Audit Manager. Inoltre, la raccolta delle prove si interrompe per tutte le valutazioni esistenti create dall'account di gestione. Audit Manager 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 (console)

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 (AWS CLI)

Esegui il comando [register-organization-admin-account](#) e utilizza il parametro `--admin-account-id` per specificare l'ID account dell'amministratore delegato.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Per aggiungere un amministratore delegato corrente (API)

Richiama l'operazione [RegisterOrganizationAdminAccount](#) e utilizza il parametro [AdminAccountID](#) per specificare l'ID account dell'amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWS specifici della lingua.

Per modificare un amministratore delegato

È possibile modificare un amministratore delegato utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

Warning

Quando modifichi un amministratore delegato, continui ad avere accesso alle prove raccolte in precedenza con il vecchio account amministratore delegato. Tuttavia, Audit Manager smette di raccogliere e allegare prove al vecchio account amministratore delegato.

Audit Manager console

Per modificare l'amministratore delegato corrente (console)

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 Audit Manager 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 di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi rimane nel loro 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

Prima di iniziare

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 Audit Manager 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 di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi rimane nel loro account A e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

Per cambiare l'attuale amministratore delegato (AWS CLI)

Prima, esegui il comando [register-organization-admin-account](#) e utilizza il parametro `--admin-account-id` per specificare l'ID account dell'amministratore delegato.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

Quindi, esegui il comando [register-organization-admin-account](#) utilizzando il parametro `--admin-account-id` per specificare l'ID account del nuovo amministratore delegato.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Prima di iniziare

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 Audit Manager 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 di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi rimane nel loro account A e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

Per cambiare l'attuale amministratore delegato (API)

Prima, esegui l'operazione [DeregisterOrganizationAdminAccount](#) e utilizza il parametro [adminAccountid](#) per specificare l'ID account dell'attuale amministratore delegato.

Quindi, richiama l'operazione [RegisterOrganizationAdminAccount](#) e utilizza il parametro [adminAccount](#) per specificare l'ID account del nuovo amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWS specifici della lingua.

Rimozione di un amministratore delegato

È possibile rimuovere un amministratore delegato utilizzando la console Audit Manager, AWS Command Line Interface (AWS CLI) o l'API Audit Manager.

⚠ Warning

Quando rimuovi un amministratore delegato, continui ad avere accesso alle prove raccolte in precedenza con l'account amministratore delegato. Tuttavia, Audit Manager smette di raccogliere e allegare prove al vecchio account amministratore delegato.

Audit Manager console

Per rimuovere l'amministratore delegato attuale (console)

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 Audit Manager 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'archivio di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi 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

Prima di iniziare

Se l'attuale amministratore delegato ha abilitato evidence finder, esegui la seguente attività di pulizia:

Assicurati che l'attuale account amministratore delegato acceda a Audit Manager 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'archivio di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi rimane nel loro account e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

Per rimuovere l'attuale amministratore delegato (AWS CLI)

Esegui il comando [deregister-organization-admin-account](#) e utilizza il parametro `--admin-account-id` per specificare l'ID account dell'amministratore delegato.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Prima di iniziare

Se l'attuale amministratore delegato ha abilitato evidence finder, esegui la seguente attività di pulizia:

Assicurati che l'attuale account amministratore delegato acceda a Audit Manager 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'archivio di dati degli eventi](#). In caso contrario, l'archivio di dati degli eventi rimane nel loro account e continua a incorrere nei costi di archiviazione di CloudTrail Lake.

Per rimuovere l'attuale amministratore delegato (API)

Richiama l'operazione [DeregisterOrganizationAdminAccount](#) e utilizza il parametro [AdminAccountId](#) per specificare l'ID account dell'amministratore delegato.

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWS specifici della lingua.

AWS Config (facoltativo)

È possibile consentire all'Audit Manager di raccogliere i risultati da AWS Config. Quando AWS Config è abilitato, Audit Manager può acquisire snapshot del livello di sicurezza delle risorse riportando i risultati dei controlli delle regole direttamente da AWS Config. Ti consigliamo di abilitare AWS Config per un'esperienza ottimale in Audit Manager.

Per abilitare AWS Config, scegli **Abilita AWS Config** per accedere a quel servizio. Per istruzioni su come abilitare AWS Config, consulta [Configurazione AWS Config](#) nella Guida per sviluppatori di AWS Config.

Security Hub (facoltativo)

È possibile consentire all'Audit Manager di importare prove AWS Security Hub per gli standard di conformità supportati. Quando Security Hub è abilitato, Audit Manager può acquisire snapshot del livello di sicurezza delle risorse in base ai risultati dei controlli di sicurezza direttamente da Security Hub. Ti consigliamo di abilitare Security Hub per un'esperienza ottimale in Audit Manager.

Per abilitare Security Hub, scegli **Abilita Security Hub** per accedere a quel servizio. Per istruzioni su come abilitare Security Hub, consulta [Configurazione di AWS Security Hub](#) nella Guida per l'utente di Security Hub.

Disabilita AWS Audit Manager

È possibile disabilitare Audit Manager se non desideri più utilizzare il servizio. Quando disabiliti Audit Manager, hai anche la possibilità di eliminare tutti i tuoi dati.

Per impostazione predefinita, quando si disabilita Audit Manager, i dati non vengono eliminati. I dati relativi alle prove vengono conservati per due anni dal momento della loro creazione. Le altre risorse di Audit Manager (incluse valutazioni, controlli personalizzati e framework personalizzati) vengono conservate a tempo indeterminato e saranno disponibili se riabiliterai Audit Manager 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, Audit Manager elimina tutti i dati relativi alle prove insieme a tutte le risorse di Audit Manager che hai creato (incluse valutazioni, controlli personalizzati e framework personalizzati). Tutti i dati vengono eliminati entro sette giorni dalla disattivazione dell'Audit Manager.

Warning

- Quando disabiliti Audit Manager, l'accesso viene revocato e il servizio non raccoglie più prove per le valutazioni esistenti. Se non riattivi Audit Manager, nessun contenuto del servizio sarà più disponibile.
- L'eliminazione di tutti i dati è un'azione permanente. Se deciderai di riattivare Audit Manager in futuro, i tuoi dati non saranno recuperabili.

È possibile disabilitare Audit Manager utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI) o l'API Audit Manager.

Audit Manager console

Per disabilitare Audit Manager (console)

1. Dalla scheda Impostazioni generali, vai alla sezione DisabilitaAWS 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 Audit Manager.
 - 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 Audit Manager a tempo indeterminato.
 - iii. Per eliminare i dati, attiva Elimina tutti i dati.
 - iv. Scegli Disabilita, quindi Disabilita Audit Manager per confermare la scelta.

AWS CLI

Prima di iniziare

Prima di disabilitare Audit Manager, puoi eseguire il comando [update-settings](#) per impostare la tua politica di conservazione dei dati preferita. Per impostazione predefinita, Audit Manager

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 (AWS CLI)

Quando sei pronto a disabilitare Audit Manager, esegui il comando [deregister-account](#).

```
aws auditmanager deregister-account
```

Audit Manager API

Prima di iniziare

Prima di disabilitare Audit Manager, puoi eseguire l'operazione API [UpdateSettings](#) per impostare la tua policy di conservazione dei dati preferita. Per impostazione predefinita, Audit Manager conserva i dati. Se desideri eliminare i tuoi dati, puoi utilizzare l'attributo [DeregistrationPolicy](#) per richiedere l'eliminazione dei tuoi dati.

Per disabilitare Audit Manager (API)

Quando sei pronto per disabilitare Audit Manager, richiama l'operazione [DeregisterAccount](#).

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare queste operazioni e parametri in uno degli SDK AWS specifici della lingua.

Per riattivare Audit Manager dopo averlo disabilitato

Vai alla home page del servizio Audit Manager e segui i passaggi per configurare Audit Manager come nuovo utente. Per ulteriori informazioni, consulta [Configurazione AWS Audit Manager](#).

Tip

- Se hai scelto di eliminare i tuoi dati quando hai disabilitato Audit Manager, 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 Audit Manager 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 Audit Manager, 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.

Impostazioni di valutazione

Utilizza questa scheda per rivedere e aggiornare le impostazioni di valutazione.

Argomenti

- [Proprietari di audit predefiniti \(opzionale\)](#)
- [Destinazione del rapporto di valutazione \(opzionale\)](#)
- [Notifiche \(facoltativo\)](#)

Proprietari di audit predefiniti (opzionale)

Puoi specificare i proprietari di audit predefiniti che hanno accesso principale alle valutazioni in Audit Manager.

Puoi 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 gli Account AWS elencati nella tabella o utilizzare la barra di ricerca per cercare altri Account AWS.

Per aggiornare le impostazioni predefinite dei proprietari dell'audit (console)

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 le impostazioni predefinite dei proprietari dell'audit (AWS CLI)

Esegui il comando [update-settings](#) e utilizza il parametro `--default-process-owners` per specificare il proprietario dell'audit.

Nell'esempio seguente, sostituisci il *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 le impostazioni predefinite dei proprietari dell'audit (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [defaultProcessOwners](#) per specificare i proprietari audit predefiniti. Nota che `roleType` può essere solo `PROCESS_OWNER`.

Per ulteriori informazioni sui proprietari degli audit, vedere [Proprietari degli audit](#) nella sezione Concetti e terminologia di questa guida.

Destinazione del rapporto di valutazione (opzionale)

Quando generi un report di valutazione, Audit Manager pubblica il report nel bucket S3 di tua scelta. Questo bucket S3 viene definito come destinazione del rapporto di valutazione. Puoi scegliere il bucket Amazon S3 in cui Audit Manager archivia i report di valutazione.

Puoi 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 destinazione del rapporto di valutazione (console)

1. Dalla scheda Impostazioni di valutazione, vai alla sezione Destinazione del rapporto di valutazione.
2. Per utilizzare un bucket Amazon S3 esistente, seleziona un nome di bucket nel menu a discesa.

3. Per creare un nuovo bucket Amazon S3, selezionare Crea un nuovo bucket.
4. Al termine, scegli Salva.

AWS CLI

Per aggiornare le impostazioni di destinazione del rapporto di valutazione (AWS CLI)

Esegui il comando [update-settings](#) e usa il parametro `--default-assessment-reports-destination` per specificare un bucket S3.

Nell'esempio seguente, sostituisci il *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 le impostazioni di destinazione del rapporto di valutazione (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [defaultAssessmentReportsDestination](#) per specificare un bucket S3.

Per istruzioni su come creare un bucket S3, vedi [Crea un bucket](#) nella Guida Utente Amazon S3.

Suggerimenti di configurazione per la destinazione del rapporto di valutazione

Per garantire la corretta generazione del rapporto di valutazione, si consiglia di verificare 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 della chiave gestita dal cliente (se ne hai fornita una) deve corrispondere alla regione di valutazione e al bucket S3 di destinazione del rapporto di valutazione. Per istruzioni su come modificare la chiave KMS, consulta [Impostazioni AWS Audit Manager, Crittografia dei](#)

[dati](#). Per istruzioni su come modificare il bucket S3, consulta [Impostazioni AWS Audit Manager, Destinazione del rapporto di valutazione](#). Per un elenco delle Regioni supportate Amazon Web, consulta la sezione [Endpoint e quote AWS Audit Manager](#) nei 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 Audit Manager. Se non hai configurato una chiave KMS nelle impostazioni di Audit Manager 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 [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 Audit Manager. È possibile specificare un bucket tra più account come destinazione del rapporto di valutazione utilizzando AWS CLI o uno degli SDK AWS, 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 del Account AWS che carica l'oggetto. 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 all'Audit Manager 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/*"
      ]
    }
  ]
}
```

Notifiche (facoltativo)

Audit Manager può inviare notifiche all'argomento Amazon SNS specificato in questa impostazione. Se sei abbonato a quell'argomento SNS, ricevi notifiche quando accedi a Audit Manager.

Puoi 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 (console)

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 (AWS CLI)

Esegui il comando [aggiorna le impostazioni](#) e usa il parametro `--sns-topic` per specificare un argomento SNS.

Nell'esempio seguente, sostituisci il *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 (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [snsTopic](#) per specificare un argomento SNS.

Note

È possibile utilizzare un argomento SNS standard o un argomento SNS FIFO (first-in-first-out). Sebbene Audit Manager supporti l'invio di notifiche agli argomenti FIFO, l'ordine in cui vengono inviati i messaggi non è garantito.

Se desideri utilizzare un argomento Amazon SNS di cui non sei proprietario, configura la policy AWS Identity and Access Management (IAM) a tale scopo. In particolare, devi configurarla per consentire la pubblicazione dal nome della risorsa Amazon (ARN)

dell'argomento. Per ulteriori informazioni su IAM, consulta [Identity and access management per AWS Audit Manager](#).

Per ulteriori informazioni sull'elenco delle azioni che richiamano le notifiche in Audit Manager, consulta [Notifiche in AWS Audit Manager](#).

Per informazioni sulla creazione di un argomento Amazon SNS, consulta [Creazione di un argomento Amazon SNS](#) nella Guida per l'utente di Amazon SNS.

Impostazioni di evidence finder

Utilizza questa scheda per rivedere e aggiornare le impostazioni di evidence finder.

Argomenti

- [Strumento evidence finder \(opzionale\)](#)
- [Destinazione di esportazione \(facoltativo\)](#)

Strumento evidence finder (opzionale)

Ti consigliamo di abilitare la funzione Ricerca prove. L'attivazione di questa funzionalità è necessaria se desideri eseguire query di ricerca sulle prove.

Segui questi passaggi per abilitare, disabilitare o controllare lo stato di evidence finder.

Abilita Evidence finder

È necessario abilitare lo strumento evidence finder in ciascuna Regione AWS in cui si desidera cercare le prove. Se sei un amministratore delegato per Audit Manager, abilita evidence finder per cercare prove per tutti gli account dei membri della tua organizzazione.

Autorizzazioni necessarie per abilitare evidence finder

Per abilitare evidence finder, sono necessarie le autorizzazioni per creare e gestire un archivio dati di eventi in CloudTrail Lake. Per utilizzare la funzionalità, sono necessarie le autorizzazioni per eseguire le query su CloudTrail Lake. Per un esempio di politica di autorizzazione che puoi utilizzare, vedi [Consentire l'accesso completo all'amministratore](#).

Per ulteriore assistenza con le autorizzazioni, contatta l'amministratore AWS. Se sei un amministratore AWS, puoi copiare la dichiarazione di autorizzazione richiesta e [allegarla a una policy IAM](#).

Richiesta di attivazione di evidence finder

Puoi completare questa attività utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI), o l'API Audit Manager.

Audit Manager console

Per richiedere l'attivazione di evidence finder (console)

1. Apri la console di Gestione audit AWS Audit all'[indirizzo https://console.aws.amazon.com/auditmanager/home](https://console.aws.amazon.com/auditmanager/home).
2. Dalla scheda delle impostazioni di Evidence finder, vai alla sezione Evidence finder.
3. Scegli Politica di autorizzazione richiesta, quindi Visualizza le autorizzazioni di 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 (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 l'attivazione di evidence finder (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [evidenceFinderEnabled](#).

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWSspecifici della lingua.

Conferma lo stato di evidence finder

Dopo aver inviato la richiesta, sono necessari fino a 10 minuti per abilitare evidence finder e creare un archivio di dati degli 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.

È possibile verificare lo stato attuale di evidence finder utilizzando la console Audit Manager, AWS CLI, o l'API Audit Manager.

Audit Manager console

Per visualizzare lo stato attuale di evidence finder (console)

1. Apri la console di Gestione audit AWS Audit all'[indirizzo https://console.aws.amazon.com/auditmanager/home](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:

- Evidence finder non è abilitato: non hai ancora abilitato evidence finder correttamente.
- Hai richiesto di abilitare evidence finder: la tua richiesta è in attesa della creazione dell'archivio di dati degli eventi
- Lo strumento di evidence finder è abilitato: l'archivio di 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 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 disabilitare evidence finder: la tua richiesta è in attesa che l'archivio di dati degli eventi venga eliminato.
- Evidence finder è stato disabilitato: Evidence finder è stato disabilitato in modo permanente e l'archivio di dati degli eventi è stato eliminato.

AWS CLI

Per visualizzare lo stato corrente di evidence finder (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 corrente di evidence finder (API)

Richiama l'operazione [OttieniImpostazioni](#) con il parametro `attribute` 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 lo strumento 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 e evidence finder risulta 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 [evidenceFinderEnablement](#) nel riferimento all'API Audit Manager.

Disattiva evidence finder

Se non desideri più utilizzare evidence finder, puoi disabilitare questa funzione in qualsiasi momento.

⚠ Warning

Disabilitare evidence finder elimina l'archivio di dati degli eventi CloudTrail Lake creato da Audit Manager. Di conseguenza, non puoi riattivare la funzione. Per riutilizzare evidence finder dopo averlo disabilitato, devi [disabilitare AWS Audit Manager](#) e quindi [riattivare](#) completamente il servizio.

Autorizzazioni necessarie per disabilitare evidence finder

Per disabilitare evidence finder, sono necessarie le autorizzazioni per eliminare l'archivio di dati degli eventi in CloudTrail Lake. Per un esempio di policy che puoi utilizzare, consulta [Autorizzazioni per disabilitare evidence finder](#).

Per ulteriore assistenza con le autorizzazioni, contatta l'amministratore AWS. Se sei un amministratore AWS, puoi [allegare la dichiarazione di autorizzazione richiesta per una policy IAM](#).

Disabilitare evidence finder

Puoi completare questa attività utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI), o l'API Audit Manager.

Audit Manager console

Per disabilitare evidence finder (console)

1. Nella sezione Evidence finder della pagina delle impostazioni di Audit Manager, scegli Disabilita.
2. Nella finestra a comparsa che appare, inserisci **Yes** per confermare la decisione.
3. Scegli Richiedi di disabilitare.

AWS CLI

Per disabilitare evidence finder (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 (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [evidenceFinderEnabled](#).

Per ulteriori informazioni, scegli i link precedenti per saperne di più nella Documentazione di riferimento dell'API AWS Audit Manager. Ciò include informazioni su come utilizzare questa operazione e questo parametro in uno degli SDK AWSspecifici della lingua.

Destinazione di esportazione (facoltativo)

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 Audit Manager salva i file esportati.

Puoi aggiornare questa impostazione utilizzando la console Audit Manager, AWS Command Line Interface(AWS CLI) o l'API Audit Manager.

Important

Il bucket S3 deve disporre della policy di autorizzazioni richiesta per consentire a CloudTrail di scrivere i file di esportazione al suo interno. Più specificamente, la policy del bucket deve includere un'azione `s3:PutObject` e l'ARN del bucket, ed elencare CloudTrail come servizio principale. 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, vedi i [suggerimenti di configurazione per la destinazione di esportazione](#) in questa pagina.

Audit Manager console

Per aggiornare le impostazioni della destinazione di esportazione (console)

1. Dalla scheda delle impostazioni di Evidence finder, vai alla sezione Destinazione di esportazione.
2. Seleziona 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**). Audit Manager 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 (AWS CLI)

Esegui il comando [update-settings](#) e usa il parametro `--default-export-destination` per specificare un bucket S3.

Nell'esempio seguente, sostituisci il *testo segnaposto* con le tue informazioni:

```
aws auditmanager update-settings --default-export-destination
destinationType=S3,destination=s3://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 (API)

Richiama l'operazione [UpdateSettings](#) e utilizza il parametro [defaultExportDestination](#) per specificare un bucket S3.

Per istruzioni su come creare un bucket S3, vedi [CreateBucket](#) nella Documentazione di riferimento delle API Amazon S3.

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

Il Regione AWS della tua 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 Audit Manager](#).

Bucket S3 multi-account

L'utilizzo di un bucket S3 per più account come destinazione dell'esportazione non è supportato nella console Audit Manager. È possibile specificare un bucket tra più account utilizzando AWS CLI o uno degli SDK AWS, 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 del Account AWS che ha caricato l'oggetto. 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 pubblici 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 all'Audit Manager 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 Principale 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/*"
      ]
    }
  ]
}
```


Notifiche in AWS Audit Manager

AWS Audit Manager può inviare notifiche sulle azioni degli utenti tramite [Amazon Simple Notification Service \(Amazon SNS\)](#).

Audit Manager 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.

Prerequisiti

Prima di configurare le notifiche Amazon SNS in Audit Manager, è necessario completare la procedura illustrata qui.

1. Crea un argomento in Amazon SNS se non ne ha già uno. Per le istruzioni, consulta la sezione [Creazione di un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.
2. Effettua la sottoscrizione di almeno un endpoint per l'argomento. Se, ad esempio, desideri ricevere notifiche tramite messaggio di testo, effettua la sottoscrizione di un endpoint SMS per l'argomento. Un endpoint SMS è un numero di cellulare. Per ricevere le notifiche tramite e-mail, effettua la sottoscrizione di un endpoint e-mail per l'argomento. Un endpoint e-mail è un indirizzo e-mail;

Per ulteriori informazioni, consulta [Nozioni di base](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

3. (Facoltativo) Se l'argomento utilizza AWS Key Management Service(AWS KMS) per la crittografia lato server (SEE), devi aggiungere autorizzazioni alla policy AWS KMS key. Per un esempio di politica che puoi utilizzare, consulta [Autorizzazioni per una chiave KMS allegata a un argomento SNS](#).

Configurazione delle notifiche in AWS Audit Manager

Segui questi passaggi per configurare le notifiche in AWS Audit Manager.

Per configurare le notifiche in AWS Audit Manager

1. Apri la console Gestione audit AWS all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. In Notifiche - facoltativo, specifica l'argomento SNS che desideri usare per ricevere le notifiche.
 - Per utilizzare un argomento esistente, seleziona il nome dell'argomento nel menu a discesa.
 - Per creare un nuovo argomento, scegli Crea nuovo argomento. Verrai indirizzato alla console Amazon SNS dove puoi creare un argomento.
4. Al termine, scegliere Save (Salva).

Note

- Puoi usare un argomento SNS standard o un argomento FIFO (first-in-first-out) SNS. Audit Manager supporta l'invio di notifiche agli argomenti FIFO. Tuttavia, l'ordine in cui vengono inviati i messaggi non è garantito.
- Se desideri utilizzare un argomento Amazon SNS di cui non sei proprietario, devi configurare la policy AWS Identity and Access Management(IAM). In particolare, devi configurare la tua policy per permettere la pubblicazione dal nome della risorsa Amazon (ARN) dell'argomento. Per ulteriori informazioni, consulta [Identity and Access Management per AWS Audit Manager](#).

Risoluzione dei problemi

Per trovare risposte a domande e problemi comuni, vedi [Risoluzione dei problemi relativi alle notifiche](#) nella sezione Risoluzione dei problemi di questa guida.

Risoluzione dei problemi in AWS Audit Manager

È possibile utilizzare le seguenti informazioni per risolvere i problemi che si verificano durante l'utilizzo di AWS Audit Manager.

Se i problemi riscontrati non rientrano nell'ambito delle seguenti informazioni, oppure persistono anche dopo che hai provato a risolverli, contatta [AWS Support](#).

Argomenti

- [Risoluzione dei problemi di valutazione e raccolta di prove](#)
- [Risoluzione dei problemi relativi ai report di valutazione](#)
- [Risoluzione dei problemi relativi ai controlli e ai set di controlli](#)
- [Risoluzione dei problemi della dashboard](#)
- [Risoluzione dei problemi relativi ad amministratori delegati e AWS Organizations](#)
- [Risoluzione dei problemi in Evidence Finder](#)
- [Risoluzione dei problemi di condivisione del framework](#)
- [Risoluzione dei problemi di notifica](#)
- [Risoluzione dei problemi di autorizzazione e accesso](#)

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 Audit Manager.

Argomenti

- [Ho creato una valutazione ma non riesco ancora a visualizzare alcuna prova](#)
- [La mia valutazione non sta raccogliendo prove di verifica della conformità da AWS Security Hub](#)
- [Ho disabilitato un controllo di sicurezza in Security Hub. Audit Manager raccoglie le prove dei controlli di conformità per quel controllo di sicurezza?](#)
- [Ho impostato lo stato di un risultato su Suppressed Security Hub. Audit Manager raccoglie prove di verifica della conformità relative a tale risultato?](#)
- [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](#)
- [La mia valutazione non sta raccogliendo prove da un altro Servizio AWS](#)
- [Le mie prove vengono generate a intervalli diversi e non sono sicuro della frequenza con cui vengono raccolte](#)
- [Cosa succede se rimuovo un account in ambito dalla mia organizzazione?](#)
- [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?](#)
- [La creazione della mia valutazione non è riuscita](#)
- [Ho disabilitato e poi riabilitato Audit Manager e ora le mie valutazioni preesistenti non raccolgono più prove](#)

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.

Assicurati di aver abilitato Security Hub e di aver configurato le impostazioni come segue.

Conferma delle impostazioni del Security Hub per un singolo Account AWS

Se ne usi uno Account AWS, controlla quanto segue:

- Conferma di aver [abilitato AWS Config e configurato la registrazione delle risorse per il tuo account](#).
- Conferma di aver [abilitato lo standard di sicurezza PCI DSS per il tuo account](#).
- Conferma di aver [attivato l'impostazione degli esiti del controllo consolidati in Security Hub](#).

Conferma delle impostazioni di Security Hub per un'organizzazione

Se utilizzi Organizations, controlla quanto segue:

- Conferma di aver [abilitato AWS Config e configurato la registrazione delle risorse per la tua organizzazione](#).
- Conferma di aver [abilitato lo standard di sicurezza PCI DSS per ogni account membro dell'organizzazione](#).
- Conferma di aver [attivato l'impostazione degli esiti del controllo consolidati in Security Hub](#).
- Verifica che l'[account di amministratore delegato utilizzato in Security Hub](#) sia lo stesso utilizzato in Audit Manager.
- Verifica di aver [abilitato gli account della tua organizzazione come account membri di Security Hub](#).

Un nome di controllo di Security Hub è stato inserito erroneamente nel tuo

ControlMappingSource

Quando utilizzi l'API Audit Manager 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 immettere 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, Audit Manager 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 delle [parole chiave di controllo di Security Hub supportate](#).

AuditManagerSecurityHubFindingsReceiverManca EventBridge la regola di Amazon

Quando abiliti Audit Manager, una regola denominata `AuditManagerSecurityHubFindingsReceiver` viene automaticamente creata e abilitata in Amazon EventBridge. Questa regola consente ad Audit Manager 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 Audit Manager](#) e quindi riattivare il servizio. Se questa azione non risolve il problema o se la disabilitazione di Audit Manager non è un'opzione, [contatta AWS Support](#) per 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, Audit Manager 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, Audit Manager 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 Config](#) per 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, Audit Manager non raccoglie prove dalla maggior parte delle [regole collegate ai servizi](#).

Esistono solo due tipi di regole collegate ai servizi da cui Audit Manager raccoglie prove:

- Regole collegate ai servizi di Conformance Pack
- Regole collegate ai servizi di AWS Organizations

Audit Manager 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 Audit Manager non raccoglie prove dalla maggior parte delle regole AWS Config collegate ai servizi è quello di evitare prove duplicate nelle valutazioni. Una regola collegata al servizio è un tipo specifico di regola gestita che consente ad altri di Servizi AWS creare AWS Config regole nell'account. 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, Audit Manager ignora la regola collegata ai servizi e non raccoglie prove da essa.

AWS Config non è abilitato e incluso come servizio nell'ambito

AWS Config deve essere abilitato nel tuo Account AWS. Inoltre, deve essere incluso come servizio in ambito per la tua valutazione. 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.

Innanzitutto, assicurati di aver abilitato AWS Config il tuo Account AWS. Per istruzioni, consulta [Abilita e configura AWS Config](#).

Quindi, assicurati di averlo incluso AWS Config come servizio nell'ambito della valutazione. Per rivedere l'elenco dei servizi in ambito per la tua valutazione, consulta la scheda [Servizi AWS Rivedi una valutazione](#). Per modificare l'elenco dei servizi che rientrano nell'ambito di una valutazione, consulta [Modifica Servizi AWS nell'ambito](#).

La AWS Config regola ha valutato una configurazione delle risorse 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 Audit Manager. In questo caso, Audit Manager 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`. `ControlMappingSource keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. Se lo inserisci in modo errato, Audit Manager 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`. `ControlMappingSource keywordValue` prevede la distinzione tra lettere maiuscole e minuscole. In caso di inserimento errato, Audit Manager 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 delle [chiamate API supportate](#).

La mia valutazione non sta raccogliendo prove da un altro Servizio AWS

Se Servizio AWS non viene selezionato nell'ambito della valutazione, Audit Manager non raccoglie prove dalle risorse relative a quel servizio. Questo vale anche se un Servizio AWS è selezionato ma non lo hai abilitato nel tuo ambiente.

Se hai creato la tua valutazione a partire da un framework personalizzato, puoi [modificare i servizi in ambito per la tua valutazione](#). È quindi possibile specificare altri elementi da Servizi AWS cui si desidera raccogliere prove. Dopo aver aggiunto questi servizi, le prove diventano disponibili dopo 24 ore.

Note

Se hai creato la valutazione partendo da un framework standard, l'elenco degli Servizi AWS in ambito è preselezionato e non può essere modificato. Questo perché quando crei una valutazione da un framework standard, Audit Manager mappa e seleziona automaticamente le origini dati e i servizi pertinenti per te. La selezione viene effettuata in base ai requisiti del framework standard. Tieni presente che, per i framework standard che contengono solo controlli manuali, non Servizi AWS rientrano nell'ambito di applicazione.

La soluzione alternativa per modificare l'ambito di applicazione pur continuando Servizi AWS a creare una valutazione basata su un framework standard consiste nel [personalizzare il framework standard](#). Ricorrendo a questa soluzione alternativa, puoi utilizzare il framework personalizzato per [creare una nuova valutazione](#). In questa valutazione, potrai specificare quali Servizi AWS siano in ambito.

Le mie prove vengono generate a intervalli diversi e non sono sicuro della frequenza con cui vengono raccolte

I controlli nelle valutazioni di Audit Manager 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)	Audit Manager 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 livello 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	Audit Manager 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, consulta [Origini dati di controllo supportate per prove automatiche](#) e [Modifica della frequenza di raccolta delle prove per un controllo](#).

Cosa succede se rimuovo un account in ambito dalla mia organizzazione?

Quando un account in ambito viene rimosso dall'organizzazione, Audit Manager 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 in ambito.

Non riesco a modificare i servizi in ambito per la mia valutazione

Quando si utilizza la console Audit Manager per creare una valutazione da un framework standard, l'elenco degli Servizi AWS ambiti inclusi viene selezionato per impostazione predefinita. L'elenco non può essere modificato. Questo perché Audit Manager mappa e seleziona automaticamente le origini dati e i servizi per te. La selezione viene effettuata in base ai requisiti del framework standard. Se il framework standard selezionato contiene solo controlli manuali, nessuno Servizi AWS rientra nell'ambito della valutazione e non è possibile aggiungere alcun servizio alla valutazione.

Se è necessario modificare l'elenco dei servizi inclusi nell'ambito, utilizzare l'operazione [UpdateAssessment](#) API fornita da Audit Manager. In alternativa, puoi [personalizzare il framework standard](#) e creare una valutazione dal framework personalizzato.

Qual è la differenza tra un servizio in ambito e un tipo di origine dati?

Un [servizio compreso nell'ambito](#) Servizio AWS è un servizio specificato come parte della valutazione. Quando un servizio è in ambito, Audit Manager raccoglie prove sull'utilizzo di quel servizio e delle sue risorse da parte tua.

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 Audit Manager 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 dell'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:

- Il [servizio in ambito](#) 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:

- Il [servizio in ambito](#) 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

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.

Ho disabilitato e poi riabilitato Audit Manager e ora le mie valutazioni preesistenti non raccolgono più prove

Quando disabiliti Audit Manager 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 Audit Manager, 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.

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 Audit Manager.

Argomenti

- [Il report di valutazione non è stato generato](#)
- [Ho seguito l'elenco di controllo sopra riportato e il mio report di valutazione non è ancora stato generato](#)
- [Ricevo un errore di accesso negato quando provo a generare un report](#)
- [Non riesco a decomprimere il report di valutazione](#)
- [Quando scelgo il nome di una prova in un report, non vengo reindirizzato ai dettagli della prova](#)
- [La generazione del mio report di valutazione è bloccata nello stato In corso e non so come ciò influisca sulla mia fatturazione](#)
- [Consulta anche](#)

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 [Impostazioni AWS Audit Manager per la 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 [Impostazioni AWS Audit Manager per la crittografia dei dati](#). Per istruzioni su come modificare il bucket S3, consulta [Impostazioni AWS Audit Manager , Destinazione del report 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. Per istruzioni su come specificare un bucket S3 diverso, consulta [Impostazioni AWS Audit Manager , Destinazione del report di valutazione](#).

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 Audit Manager. Se non

hai configurato una chiave KMS nelle impostazioni di Audit Manager 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 [Impostazioni AWS Audit Manager , Crittografia dei dati](#). Per istruzioni su come modificare il bucket S3, consulta [Impostazioni AWS Audit Manager , Destinazione del report 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

Audit Manager 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 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.

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 Audit Manager. Per evitare questo errore, quando designi un amministratore delegato per Audit Manager, assicurati che il suo account abbia accesso alla chiave KMS che hai fornito durante la configurazione di Audit Manager.

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 Audit Manager 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, consulta [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 policy che puoi utilizzare, consulta Esempi di policy basate sull'identità per AWS Audit Manager](#).

Note

Se modifichi le impostazioni di crittografia dei dati di Audit Manager, 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 Audit Manager.

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](#).

Consulta anche

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 riesco ad aggiungere risultati di ricerca individuali a un report di valutazione](#)
- [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 Audit Manager.

Problemi generali

- [Non riesco a vedere alcun controllo o set di controlli nella mia valutazione](#)
- [Non riesco a caricare prove manuali su un controllo](#)

Problemi di integrazione di AWS Config

- [Devo utilizzare 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 Audit Manager?](#)

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 Audit Manager.

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 dell'audit di utilizzare la [AWSAuditManagerAdministratorAccess](#) policy. 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 ulteriori informazioni, consulta [Aggiornare lo stato dei controlli](#).

Important

Ciascuno Account AWS può caricare manualmente fino a 100 file di prove su un controllo ogni giorno. Il superamento di questa quota giornaliera fa sì che eventuali caricamenti manuali aggiuntivi non rientrino in tale controllo. Se devi caricare una grande quantità di prove manuali su un unico controllo, caricale in batch nell'arco di diversi giorni.

Devo utilizzare 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. A tale scopo, configura più origini dati per il controllo e seleziona il tipo di regola preferito per ognuna di esse. Puoi definire fino a 10 origini dati 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'[DescribeConfigRules](#) operazione 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 Audit Manager.

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-rule](#) comando.

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 Audit Manager.

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 Config](#) per 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.

	Name	Remediation action	Type	Compliance
<input type="radio"/>	account-part-of-organizations	Not set	AWS managed	✔ Compliant

Dopo aver confermato che si tratta di una regola gestita, torna in Audit Manager 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.

AWS Config rule type [Info](#)

Select a rule type to view a list of the available rules.

Managed rule
Use one of the predefined rules that are provided by AWS Config.

Custom rule
Use a custom rule that was created for your AWS account or organization.

Managed rule
For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

ACCOUNT_PART_OF_ORGANIZATIONS

Non riesco a vedere la regola gestita che voglio usare

Prima di selezionare una regola dall'elenco a discesa nella console di Audit Manager, assicurati di aver selezionato Regola gestita come tipo di regola.

AWS Config rule type [Info](#)

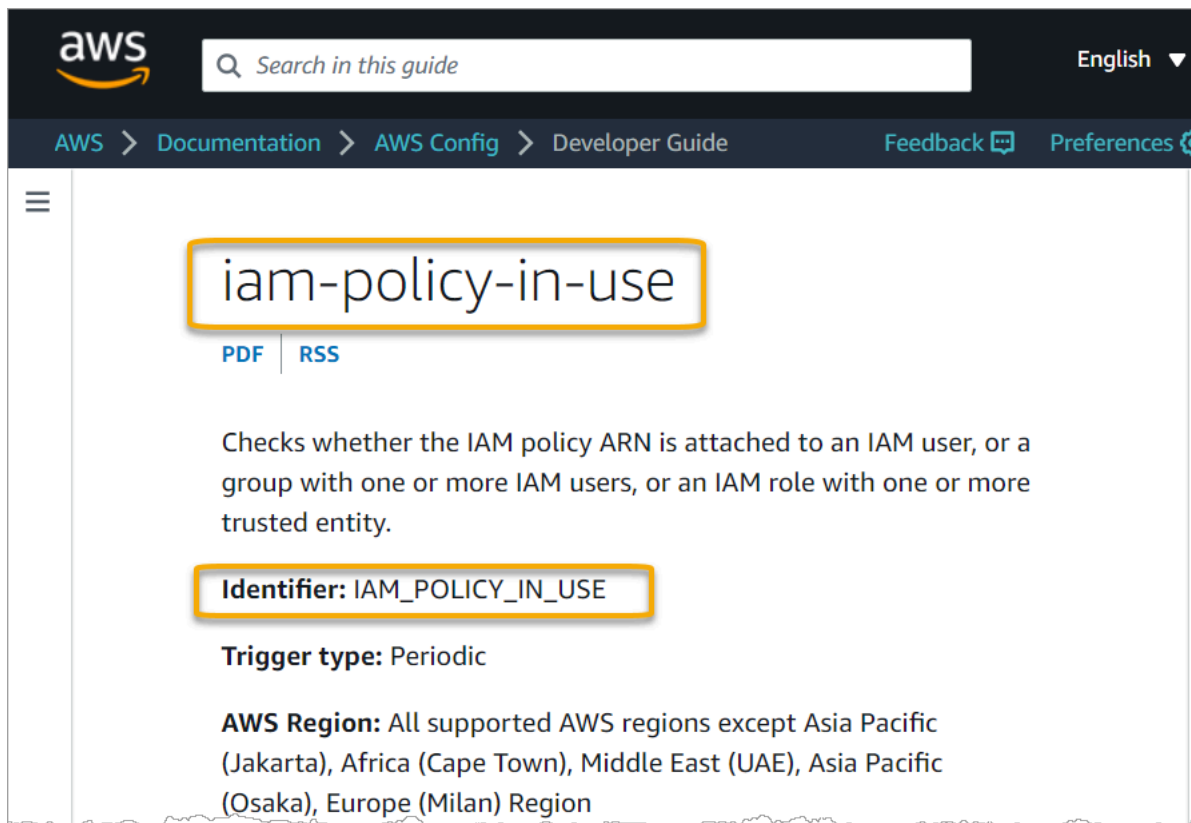
Select a rule type to view a list of the available rules.

Managed rule
Use one of the predefined rules that are provided by AWS Config.

Custom rule
Use a custom rule that was created for your AWS account or organization.

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 Audit Manager.



The screenshot shows the AWS Config documentation page for the rule `iam-policy-in-use`. The page header includes the AWS logo, a search bar, and the language set to English. The breadcrumb navigation shows the path: AWS > Documentation > AWS Config > Developer Guide. The rule name `iam-policy-in-use` is highlighted with a yellow box. Below it are links for PDF and RSS. The description states: "Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity." The identifier `Identifier: IAM_POLICY_IN_USE` is also highlighted with a yellow box. The trigger type is listed as "Trigger type: Periodic". The AWS Region is listed as "AWS Region: All supported AWS regions except Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Osaka), Europe (Milan) Region".

Se utilizzi una regola gestita personalizzata, puoi utilizzare la [console AWS Config](#) 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 di questa regola, vai alla AWS Config console, scegli Regole nel menu di navigazione a sinistra e scegli la regola nella tabella.

Rules			
<input type="text" value="Any status"/>		View details Edit rule Actions ▾ Add rule	
		< 1 2 3 > ⚙️	
Name	Remediation action	Type	
<input type="radio"/> customized-iam-policy-in-use	Not set	AWS managed	

Scegli Modifica per aprire i dettagli sulla regola gestita.

customized-iam-policy-in-use

Actions ▾

▼ **Rule details** Edit

<p>Description</p> <p>Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.</p>	<p>Trigger type</p> <p>Periodic: 24 hours</p> <p>Scope of changes</p> <p>-</p>	<p>Last successful evaluation</p> <p>🕒 Not available</p>
---	--	---

Nella sezione Dettagli, puoi trovare l'identificatore di origine da cui è stata creata la regola gestita (IAM_POLICY_IN_USE).

Edit rule

Details

Name
A unique name for the rule. 128 characters max. No special characters or spaces.

customized-iam-policy-in-use

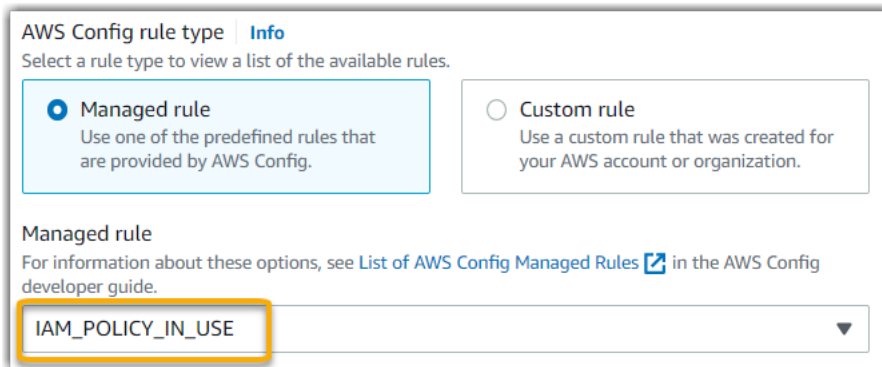
Description

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

Managed rule name

IAM_POLICY_IN_USE

È ora possibile tornare alla console di Audit Manager e selezionare la stessa parola chiave identificativa dall'elenco a discesa.



AWS Config rule type **Info**
Select a rule type to view a list of the available rules.

Managed rule
Use one of the predefined rules that are provided by AWS Config.

Custom rule
Use a custom rule that was created for your AWS account or organization.

Managed rule
For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

IAM_POLICY_IN_USE ▼

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, Audit Manager 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, Audit Manager 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 Audit Manager?

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. Audit Manager rileva e gestisce gli aggiornamenti delle regole come descritto nella tabella seguente. Audit Manager non invia notifiche quando rileva un aggiornamento delle regole.

Scenario	Cosa fa Audit Manager	Cosa devi fare tu
Una regola personalizzata viene aggiornata nell'istanza di AWS Config.	Audit Manager 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.	Audit Manager 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. In questo modo puoi ripulire le impostazioni dell'origine 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
Mittente	<ul style="list-style-type: none"> 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. 	<p>Informa il destinatario del tuo aggiornamento. In questo modo, potrà applicare lo stesso aggiornamento e rimanere sincronizzato con l'ultima definizione della regola.</p>
Destinatario	<ul style="list-style-type: none"> 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. 	<p>Aggiorna la regola corrispondente nella tua istanza di AWS Config.</p>

Risoluzione dei problemi della dashboard

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti la dashboard di Audit Manager.

Argomenti

- [Non ci sono dati nella mia dashboard](#)
- [L'opzione di download in formato CSV non è disponibile](#)
- [Non vedo il file scaricato quando cerco di scaricare un file CSV](#)
- [Nella dashboard non è presente un controllo o un dominio di controllo specifico](#)
- [Lo snapshot quotidiano mostra ogni giorno quantità diverse di prove. È normale che sia così?](#)

Non ci sono dati nella mia dashboard

Se i numeri nel [widget di snapshot giornaliero](#) sono accompagnati da un trattino (-), significa che non ci sono dati disponibili. 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.

L'opzione di download in formato CSV non è disponibile

Questa opzione è disponibile solo per le valutazioni individuali. Assicurati di aver applicato un [the section called "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 Audit Manager. 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 Audit Manager 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 sulla frequenza di raccolta delle prove, consulta [Come AWS Audit Manager raccoglie le 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 Audit Manager.

Argomenti

- [Non riesco a configurare Audit Manager con il mio account di amministratore delegato](#)
- [Quando creo una valutazione, non riesco a visualizzare gli account della mia organizzazione in Account in ambito](#)
- [Ricevo un errore di accesso negato quando provo a generare un report di valutazione utilizzando il mio account di amministratore delegato](#)
- [Cosa succede in Audit Manager se scollego un account membro dalla mia organizzazione?](#)
- [Cosa succede se ricollego un account membro alla mia organizzazione?](#)
- [Cosa succede se eseguo la migrazione di un account membro da un'organizzazione all'altra?](#)

Non riesco a configurare Audit Manager 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 Audit Manager, 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 111111111111 from 222222222222 to 333333333333

Scegli l'account individuale che desideri utilizzare come amministratore delegato in Audit Manager. Assicurati di registrare prima l'account di amministratore delegato in Organizations, quindi [aggiungi lo stesso account come amministratore delegato](#) in Audit Manager.

Quando creo una valutazione, non riesco a visualizzare gli account della mia organizzazione in Account in ambito

Se desideri che la valutazione di Audit Manager includa più account della tua organizzazione, devi specificare un amministratore delegato.

Assicurati di aver configurato un account di amministratore delegato per Audit Manager. Per istruzioni, consulta [Impostazioni, 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 Audit Manager, 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 Audit Manager. Per informazioni su come rivedere e modificare le impostazioni di crittografia, consulta [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 Audit Manager. Per evitare questo errore, quando designi un amministratore delegato per Audit Manager, assicurati che il suo account abbia accesso alla chiave KMS che hai fornito durante la configurazione di Audit Manager.

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 Audit Manager 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, consulta [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 il report di valutazione. [Per un esempio di policy che puoi utilizzare, consulta Esempi di policy basate sull'identità per AWS Audit Manager](#).

Note

Se modifichi le impostazioni di crittografia dei dati di Audit Manager, 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 Audit Manager se scollego un account membro dalla mia organizzazione?

Quando si scollega un account membro da un'organizzazione, Audit Manager riceve una notifica relativa a questo evento. Audit Manager 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 Audit Manager 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 Audit Manager non è più abilitato sul suo account.

Cosa succede se ricollego un account membro alla mia organizzazione?

Quando ricollegi un account membro alla tua organizzazione, quell'account non viene aggiunto automaticamente all'ambito delle tue valutazioni esistenti di Audit Manager. 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 [Modifica Account AWS nell'ambito](#).
- Per nuove valutazioni, puoi aggiungere l'account ricollegato durante l'impostazione della valutazione. Per istruzioni, consulta [Specificare Account AWS nell'ambito](#).

Cosa succede se eseguo la migrazione di un account membro da un'organizzazione all'altra?

Se un account membro ha Audit Manager abilitato nell'organizzazione 1 e poi migra all'organizzazione 2, Audit Manager 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 Audit Manager.

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 di query non riesce a essere eseguita.](#)
- [Altre risorse](#)

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

Se stai tentando di abilitare Evidence Finder per la prima volta, assicurati di disporre delle [autorizzazioni necessarie](#). Queste autorizzazioni 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 controllare lo stato del backfill dei dati, consulta [Conferma 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 tentando di disabilitare Evidence Finder, assicurati di disporre delle [autorizzazioni necessarie](#). Queste autorizzazioni ti consentono di aggiornare ed eliminare un archivio dati di 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'[StartQuery](#) operazione 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 Audit Manager.

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'[StartQuery](#) API 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 Audit Manager. 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, Audit Manager 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 di query non riesce a essere eseguita.

Se utilizzi l'[CreateAssessmentReport](#) API 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.

Clausola	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 Audit Manager.
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 Audit Manager	Rimuovi la clausola FROM e sostituiscila con FROM <i>edsID</i> , dove il valore di edsID corrisponde all'ID del datastore di eventi specificato nelle impostazioni di Audit Manager. Puoi recuperare l'ARN del datastore di eventi dalle tue impostazioni di Audit Manager. Per ulteriori informazioni, GetSettings consulta l'AWS Audit Manager API Reference.	Questa convalida viene gestita da Audit Manager.

Clausola	Problema	Soluzione	Note
GROUP BY	Nella query è presente una clausola GROUP BY	Rimuovi la clausola GROUP BY.	Questa convalida viene gestita da Audit Manager.
HAVING	Nella query è presente una clausola HAVING	Rimuovi la clausola HAVING.	Questa convalida viene gestita da Audit Manager.
LIMIT	La clausola LIMIT contiene un valore che supera il limite massimo consentito	<p>Se la clausola LIMIT esiste, assicurati che il suo valore sia uguale o inferiore al limite massimo supportato:</p> <ul style="list-style-type: none"> • Per i report relativi alla stessa regione, il limite è 22.000 • 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 	<p>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.</p> <p>Se non è fornito alcun valore LIMIT nell'istruzione di query, vengono applicati i limiti massimi predefiniti. Questa convalida viene gestita da Audit Manager.</p>
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

Clausol	Problema	Soluzione	Note
WHERE	<p>La clausola WHERE contiene più di una assessmentId oppure</p> <p>La clausola WHERE contiene un assessmentId che non corrisponde all'assessmentId nella tua richiesta createAssessmentReport oppure</p> <p>La clausola WHERE contiene un nome di colonna non supportato</p>	<p>Assicurati che sia specifica to un solo AssessmentID e che corrisponda al parametro AssessmentID specificato nella richiesta API createAssessmentReport .</p> <p>Rimuovi i nomi di colonna non supportati.</p>	<p>Questa convalida è gestita dall'API. CloudTrail StartQuery</p>

Esempi

Gli esempi seguenti mostrano come utilizzare il queryStatement parametro quando si chiama l'[CreateAssessmentReport](#) operazione. Prima di utilizzare queste query, sostituisci il *testo segnaposto* con i tuoi valori edsIde 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
```

Altre risorse

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 controllare lo stato del backfill, consulta [Conferma dello stato di Evidence Finder](#).

La tua query di ricerca è riuscita

Audit Manager 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, Audit Manager 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, Audit Manager non esporta risultati parziali. Per evitare un timeout, puoi ridurre la quantità di prove scansionate [modificando la query 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 Audit Manager 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` e l'ARN del bucket ed essere elencata CloudTrail come principale del servizio. Di seguito proponiamo un [esempio di policy](#) che puoi utilizzare. Per istruzioni su come utilizzare un bucket S3 diverso, consulta [impostazioni di destinazione delle esportazioni](#).

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, consulta [Impostazioni per la crittografia dei dati](#).

5. Verifica le autorizzazioni del tuo account di amministratore delegato:

- a. La chiave gestita dal cliente nelle impostazioni di Audit Manager 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 in Audit Manager, consulta [Impostazioni di crittografia dei dati](#).

Note

Quando modifichi le impostazioni di crittografia dei dati di Audit Manager, 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 CSV 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 Audit Manager. 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 di condivisione del framework

Puoi utilizzare le informazioni presentate in questa pagina per risolvere i problemi più comuni riguardanti la condivisione dei framework in Audit Manager.

Argomenti

- [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 ha 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?](#)

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 Audit Manager, 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. Audit Manager 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.

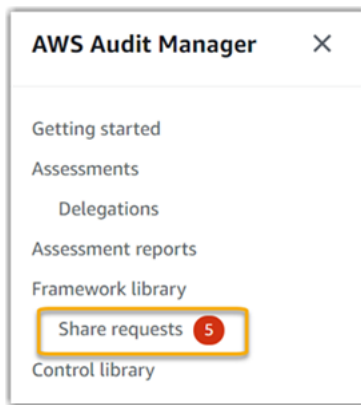
Puoi utilizzare la procedura seguente per verificare la presenza di eventuali richieste di condivisione in scadenza e inviare un promemoria facoltativo al destinatario affinché intervenga.

Per visualizzare le notifiche relative alle richieste inviate

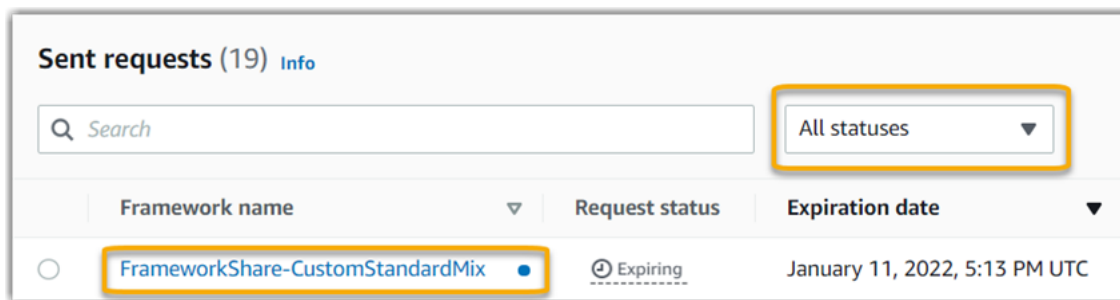
1. Apri la console di AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Se hai una notifica di richiesta di condivisione, Audit Manager visualizza un punto rosso accanto all'icona del menu di navigazione.



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 Audit Manager 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. Audit Manager 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.

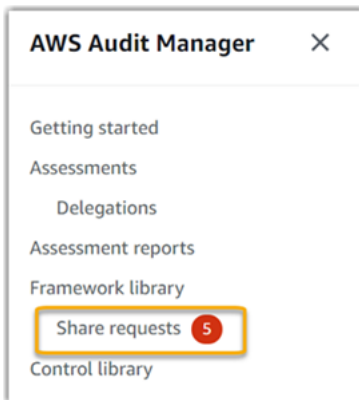
Per verificare la presenza di richieste di condivisione attive e in scadenza, utilizza la procedura indicata di seguito.

Per visualizzare le notifiche relative alle richieste ricevute

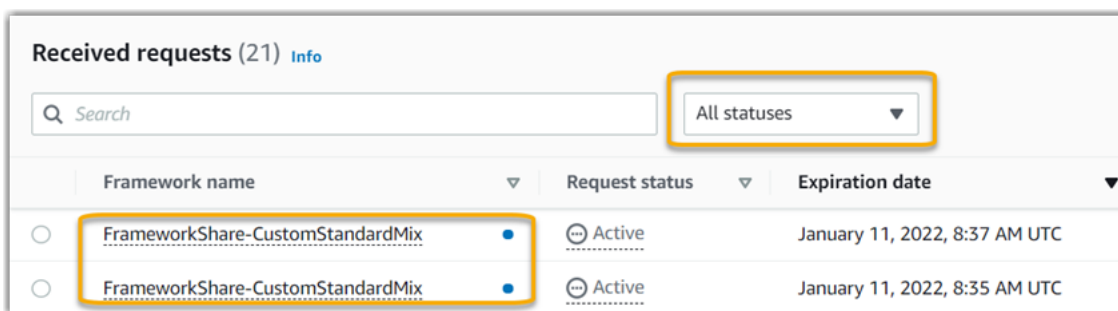
1. Apri la console di AWS Audit Manager all'indirizzo <https://console.aws.amazon.com/auditmanager/home>.
2. Se hai una notifica di richiesta di condivisione, Audit Manager visualizza un punto rosso accanto all'icona del menu di navigazione.



3. Espandi il riquadro di navigazione e guarda accanto a Condividi richieste. Un badge di notifica indica il numero di richieste di condivisione che richiedono la tua attenzione.



4. Scegli Condividi richieste. 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 ha 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, Audit Manager 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. Audit Manager rileva e gestisce gli aggiornamenti delle regole come descritto nella tabella seguente. Audit Manager non invia notifiche quando rileva un aggiornamento delle regole.

Scenario	Cosa fa Audit Manager	Cosa devi fare tu
Una regola personalizzata viene aggiornata nell'istanza di AWS Config.	Audit Manager 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.	Audit Manager interrompe la segnalazione degli esiti della regola eliminata.	Non è richiesta alcuna azione. Se lo desideri, puoi modificare e 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
Mittenti	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 Audit Manager.

Argomenti

- [Ho specificato un argomento di Amazon SNS in Audit Manager, 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 Audit Manager, 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. Un esempio di policy è disponibile nella pagina [Notifiche](#) di questa guida.
- 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

Audit Manager supporta l'invio di notifiche agli argomenti FIFO SNS. Tuttavia, l'ordine in cui Audit Manager 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 Audit Manager.

Argomenti

- [Ho seguito la procedura di configurazione di Audit Manager, ma non dispongo di privilegi IAM sufficienti](#)
- [Ho indicato qualcuno come proprietario dell'audit, ma non ha ancora pieno accesso alla valutazione. Perché?](#)
- [Non riesco a eseguire un'operazione in Audit Manager](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Audit Manager](#)
- [Consulta anche](#)

Ho seguito la procedura di configurazione di Audit Manager, ma non dispongo di privilegi IAM sufficienti

L'utente, il ruolo o il gruppo utilizzato per accedere ad Audit Manager 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. La procedura di [configurazione](#) illustrata in questa guida fornisce una policy che concede le autorizzazioni minime necessarie per configurare Audit Manager. 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 Audit Manager 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 di audit, la politica consigliata è. [AWSAuditManagerAdministratorAccess](#) Per i delegati, puoi utilizzare

[questo esempio](#), fornito 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 Audit Manager. 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, Audit Manager garantisca il pieno controllo su tutte le specifiche di ciascuna valutazione.

Note

Per i titolari degli audit, si consiglia di utilizzare la [AWSAuditManagerAdministratorAccess](#) politica. Per ulteriori informazioni, consulta [Policy consigliate per i profili utente in Audit Manager](#).

Non riesco a eseguire un'operazione in Audit Manager

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.

Voglio 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 accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Audit Manager supporti 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente IAM.

Consulta anche

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 di valutazione](#)
- [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 in Evidence Finder](#)
- [Ho specificato un argomento di Amazon SNS in Audit Manager, ma non ho ricevuto alcuna notifica](#)

Quote e restrizioni per AWS Audit Manager

Il tuo Account AWS dispone di quote predefinite, precedentemente chiamate limiti, per ogni 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, è elencata nello spazio dei nomi AWS Audit Manager nella console Service Quotas. Per sapere come richiedere un aumento delle quote, consulta [Gestione delle proprie quote di Audit Manager](#).

Quote predefinite di Audit Manager

Di seguito sono elencate le quote AWS Audit Manager per account Account AWS per regione.

Valutazioni

- Numero di valutazioni attive per account: 100

Report 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 valutazione correlata utilizza un AWS KMS key gestito dal cliente: 3.500

Controlli

- Numero di controlli personalizzati per account: 500

Prove

- 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 dei framework personalizzati condivisi

- Numero di account di destinatari attivi: 100

Accesso API

- Numero di transazioni al secondo (TPS) su tutte le API: 20 TPS

Gestione delle proprie quote di Audit Manager

AWS Audit Manager è integrato con Service Quotas, un Servizio AWS che consente di visualizzare e gestire le quote da una posizione centrale. Per ulteriori informazioni, consulta [Cos'è Service Quotas?](#) nella Guida per l'utente di Service Quotas. Service Quotas semplifica la ricerca del valore di tutte le proprie quote di Audit Manager.

Per visualizzare le quote di servizio di Audit Manager 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 Service quotas, è possibile visualizzare il nome della quota di servizio, il valore applicato (se disponibile), il valore di quota predefinito AWS 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.

Per ulteriori informazioni, consulta [Richiesta di un aumento di quota](#) nella Guida per l'utente di Service Quotas.

Sicurezza 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 gestisce AWS i servizi 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 dal AWS servizio 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 ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Audit Manager. I seguenti argomenti illustrano come configurare Audit Manager per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Audit Manager.

Argomenti

- [Protezione dei dati in AWS Audit Manager](#)
- [Gestione delle identità e degli accessi per AWS Audit Manager](#)
- [Convalida della conformità per AWS Audit Manager](#)
- [Resilienza in AWS Audit Manager](#)
- [Sicurezza dell'infrastruttura in AWS Audit Manager](#)
- [AWS Audit Manager e endpoint VPC di interfaccia \(\)AWS PrivateLink](#)
- [Registrazione e monitoraggio AWS Audit Manager](#)
- [Analisi della configurazione e della vulnerabilità in AWS Audit Manager](#)

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 Audit Manager 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 Audit Manager

Esistono vari modi per eliminare i dati Audit Manager.

Eliminazione dei dati quando si disabilita Audit Manager

Quando [disabiliti Audit Manager](#), puoi decidere se eliminare tutti i tuoi dati di Audit Manager. Se scegli di eliminare i tuoi dati, questi verranno eliminati entro 7 giorni dalla disattivazione di Audit Manager. Dopo aver eliminato i tuoi dati, non puoi recuperarli.

Eliminazione automatica dei dati

Alcuni dati di Audit Manager vengono eliminati automaticamente dopo un determinato periodo di tempo. Audit Manager 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 Audit Manager in qualsiasi momento. Per le istruzioni, consulta quanto segue:

- [Eliminazione di una valutazione](#)

- Vedi anche: [DeleteAssessment](#) nell'AWS Audit Manager API Reference
- [Eliminazione di un framework personalizzato](#)
- Vedi anche: [DeleteAssessmentFramework](#) nell'AWS Audit Manager API Reference
- [Eliminazione di una richiesta di condivisione](#)
- Vedi anche: [DeleteAssessmentFrameworkShare](#) nell'AWS Audit Manager API Reference
- [Eliminazione di un report di valutazioni](#)
- Vedi anche: [DeleteAssessmentReport](#) nell'AWS Audit Manager API Reference
- [Eliminazione di un controllo personalizzato](#)
- Vedi anche: [DeleteControl](#) nell'AWS Audit Manager API Reference

Per eliminare altri dati di risorse che potresti aver creato durante l'utilizzo di Audit Manager, 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 un Chiave di proprietà di AWS per crittografare i tuoi contenuti. Tutti i metadati di servizio in DynamoDB e Amazon S3 in Audit Manager sono crittografati utilizzando una Chiave di proprietà di AWS.

Audit Manager 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 Audit Manager 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

Audit Manager 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, Audit Manager 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 Audit Manager, 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 [Abilita AWS Audit Manager](#).

Puoi rivedere e modificare le tue impostazioni di crittografia in qualsiasi momento. Per istruzioni, consulta [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) è uno strumento Servizio AWS che aiuta un 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 Audit Manager. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come AWS Audit Manager funziona con IAM](#)
- [Esempi di policy basate sull'identità per AWS Audit Manager](#)
- [Prevenzione del confused deputy tra servizi](#)
- [AWS politiche gestite per AWS Audit Manager](#)
- [Risoluzione dei problemi di AWS Audit Manager identità e accesso](#)
- [Utilizzo di ruoli collegati ai servizi per AWS Audit Manager](#)

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 Audit Manager per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità Audit Manager 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 Amazon MQ, consulta [Risoluzione dei problemi di AWS Audit Manager identità e accesso](#).

Amministratore del servizio: se sei il responsabile delle risorse Audit Manager presso la tua azienda, probabilmente disponi dell'accesso completo a Audit Manager. Il tuo compito è determinare le caratteristiche e le risorse Audit Manager 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 Audit Manager 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 ad Audit Manager. Per visualizzare policy basate su identità Audit Manager 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 AWS](#) nella Guida per l'utente di 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. Conservare le credenziali dell'utente root e utilizzarle 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 di 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, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS 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 sul Centro identità IAM, consulta [Cos'è Centro identità IAM?](#) 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, per 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 di 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 di 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 di 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 di 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 ulteriori 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 informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di 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 un 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 AWS](#) nella Guida per l'utente di 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'operazione 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 di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di 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 di 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 azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `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 ruoli 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 di 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 di 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 utilizzarle 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 funzione 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 di 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 di 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 ad Audit Manager, scopri quali funzionalità di IAM sono disponibili per l'uso con Audit Manager.

Funzionalità IAM che puoi utilizzare con AWS Audit Manager

Funzionalità IAM	Supporto Audit Manager
Policy basate su identità	Sì
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 di 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 Audit Manager. 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 Audit Manager e le relative politiche consigliate sono definite come segue.

Utente	Descrizione e policy consigliata
Proprietario dell'audit	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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: Consenti agli utenti l'accesso completo come amministratore 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 Audit Manager, 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 utilizzarle 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 [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

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 operazioni 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 Audit Manager, consulta [Esempi di policy basate sull'identità per AWS Audit Manager](#).

Risorse politiche per AWS Audit Manager

Supporta le risorse di policy	Si
-------------------------------	----

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'azione. 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 AWS Audit Manager](#).

Una valutazione Audit Manager presenta il seguente formato nome della risorsa Amazon (ARN):

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Un set di controlli Audit Manager presenta il seguente formato ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/  
${assessmentId}controlSet/${controlSetId}
```

Un controllo Audit Manager 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 Audit Manager, 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 Audit Manager 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 Audit Manager e i relativi ARN, consulta [Risorse definite da AWS Audit Manager](#) nella 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 Audit Manager 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:SourceArno` `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:SourceArne` `aws:SourceAccount` in Audit Manager per prevenire il problema `confused deputy`.

- [Policy di esempio per un argomento SNS utilizzato per le notifiche di Audit Manager](#)
- [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.

Audit Manager 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 ad 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 di 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, consulta [Tagging delle 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 di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API o AWS CLI. 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)	Si
--	----

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 un 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 AWS](#) nella 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 Audit Manager 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'operazione 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 Manager [Utilizzo 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 Audit Manager. 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 azioni 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 AWS Audit Manager, incluso il formato degli ARN per ogni tipo di risorsa, consulta [Operazioni, risorse e chiavi di condizione per AWS Audit Manager](#) in Guida di riferimento per l'autorizzazione del servizio.

Argomenti

- [Best practice per le policy](#)

- [Consenti le autorizzazioni minime richieste per abilitare Audit Manager](#)
- [Consenti agli utenti l'accesso completo come amministratore a AWS Audit Manager](#)
- [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](#)
- [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 Audit Manager 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 AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: 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 di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni 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 di 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 di 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 di 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 Audit Manager

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 Audit Manager. Sono necessarie tutte le autorizzazioni previste nella seguente policy. Se ometti una parte di questa policy non potrai più abilitare Audit Manager.

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 Audit Manager, 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`)

Questa policy è identica alla policy gestita, `AWSAuditManagerAdministratorAccess`. Questa policy include la possibilità di abilitare e disabilitare Audit Manager, di modificare le impostazioni di Audit Manager e di gestire tutte le risorse di Audit Manager come valutazioni, framework, controlli e report di valutazione.

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

```

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 Audit Manager.

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 funzione 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 Audit Manager. 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. È possibile recuperare l'ARN dell'archivio dati degli eventi dalle impostazioni di Audit Manager. Per ulteriori informazioni, consulta [GetSettings](#) l'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 Audit Manager (valutazioni, framework e controlli), ma non garantisce la possibilità di abilitare o disabilitare Audit Manager o di modificare le impostazioni di Audit Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:CreateAssessmentFramework",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:UpdateAssessmentFramework",
        "auditmanager>DeleteAssessmentFramework",
        "auditmanager:ListAssessmentReports",

```

```

        "auditmanager:ListAssessments",
        "auditmanager:CreateAssessment",
        "auditmanager:ListControls",
        "auditmanager:CreateControl",
        "auditmanager:GetControl",
        "auditmanager:UpdateControl",
        "auditmanager>DeleteControl",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:GetDelegations",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "auditmanager:ListNotifications",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListTagsForResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource"
    ],
    "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 collegate 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:ListGroupForUser",
        "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 Audit Manager 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 policy di accesso agli argomenti SNS.
- [Esempio 2](#): se il tuo argomento SNS utilizza AWS Key Management Service (AWS KMS) per la crittografia lato server (SSE), usa questo esempio per aggiungere autorizzazioni alla politica di accesso alle chiavi KMS.

Nelle seguenti policy, il principale che ottiene le autorizzazioni è il principale del servizio, 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](#) [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 Audit Manager 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 Audit Manager 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 Audit Manager su tutte le risorse di Audit Manager. 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 `StringEqual` o `StringLike`. Come best practice, consigliamo di usare `StringEqual` 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 Audit Manager 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 `StringEqual` o `StringLike`. Come best practice, consigliamo di usare `StringEqual` 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 funzione 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 [aws:SourceArn](#) 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 Audit Manager. In questo caso, nella policy di accesso agli argomenti SNS, il valore ARN `aws:SourceArn` è la risorsa Audit Manager da cui proviene la notifica. Poiché è probabile che tu

disponga di più risorse Audit Manager, ti consigliamo di utilizzare `aws:SourceArn` con un carattere jolly. In questo modo puoi specificare tutte le risorse di Audit Manager 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` 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:service:*:123456789012:*`.

Supporto confused deputy Audit Manager

Audit Manager 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 Audit Manager](#)
- [Policy di esempio: la chiave KMS che usi per crittografare il tuo argomento SNS](#)

Audit Manager non fornisce un supporto confused deputy per la chiave gestita dal cliente fornita nelle impostazioni [Crittografia dei dati](#) di Audit Manager. 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 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 AWS](#) nella 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.

```
{
  "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 la sezione relativa all'[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 Audit Manager 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:DescribeEndpointConfig`
- `sagemaker:ListEndpointConfigs`
- `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:ListEndpointConfigs",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
```



```

    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "sagemaker:DescribeEndpointConfig",
    "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	<p>Abbiamo aggiunto le seguenti autorizzazioni a AWSAuditManagerServiceRolePolicy</p> <p>AWS Audit Manager ora puoi eseguire le seguenti azioni per raccogliere prove automatiche sulle risorse del tuo Account AWS.</p> <ul style="list-style-type: none"> iam:ListAttachedGroupPolicies iam:ListAttachedUserPolicies iam:ListGroupsForUser es:ListDomainNames <p>Abbiamo anche aggiunto una nuova risorsa nella APIGatewayAccess sezione della</p>	17/05/2024

Modifica	Descrizione	Data
	<p>politica (arn:aws:apigateway:*::/rest apis).</p> <p>La policy ora concede l'autorizzazione specifica (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.</p>	
<p>AWSAuditManagerAdministratorAccess: aggiornamento a una policy esistente</p>	<p>Abbiamo aggiunto la seguenti autorizzazione relativa a AWSAuditManagerAdministratorAccess :</p> <ul style="list-style-type: none"> • controlcatalog:ListCommonControls • controlcatalog:ListDomains • controlcatalog:ListObjectives <p>Questo aggiornamento consente di visualizzare i domini di controllo, gli obiettivi di controllo e i controlli comuni forniti da Control Catalog. AWS</p>	<p>15/05/2024</p>

Modifica	Descrizione	Data
<p>AWSAuditManagerServiceRolePolicy</p> <p>: aggiornamento a una policy esistente</p>	<p>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.</p> <ul style="list-style-type: none"> • 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 	<p>15/05/2024</p>

Modifica	Descrizione	Data
	<ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • <code>secretsmanager:DescribeSecret</code> • <code>secretsmanager:ListSecrets</code> • <code>sns:ListTagsForResource</code> • <code>waf-regional:GetRule</code> • <code>waf-regional:GetWebAcl</code> • <code>waf-regional:ListRules</code> • <code>waf:GetRule</code> • <code>waf:GetRuleGroup</code> • <code>waf:ListRuleGroups</code> • <code>waf:ListRules</code> • <code>waf:ListWebAcls</code> • <code>wafv2:ListWebAcls</code> 	
<p>AWSAuditManagerServiceRolePolicy</p> <p>: aggiornamento a una policy esistente</p>	<p>Il ruolo collegato al servizio ora consente AWS Audit Manager di eseguire l'azione. <code>s3:GetBucketPolicy</code></p> <p>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.</p> <p>L'<code>GetBucketPolicy</code> azione opera nell'ambito di Account AWS dove <code>service-linked-role</code> è disponibile. Non può accedere alle policy relative ai bucket su più account.</p>	<p>12/06/2023</p>

Modifica	Descrizione	Data
<p>AWSAuditManagerServiceRolePolicy</p> <p>: aggiornamento a una policy esistente</p>	<p>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.</p> <ul style="list-style-type: none"> • 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 	<p>11/06/2023</p>

Modifica	Descrizione	Data
	<ul style="list-style-type: none"> • <code>ec2:DescribeAddresses</code> • <code>ec2:DescribeCustomerGateways</code> • <code>ec2:DescribeEgressOnlyInternetGateways</code> • <code>ec2:DescribeInternetGateways</code> • <code>ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations</code> • <code>ec2:DescribeLocalGateways</code> • <code>ec2:DescribeLocalGatewayVirtualInterfaces</code> • <code>ec2:DescribeNatGateways</code> • <code>ec2:DescribeTransitGateways</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeVpnConnections</code> • <code>ec2:DescribeVpnGateways</code> • <code>ec2:GetEbsDefaultKmsKeyId</code> • <code>ec2:GetEbsEncryptionByDefault</code> • <code>ecs:DescribeClusters</code> • <code>eks:DescribeAddonVersions</code> • <code>elasticache:DescribeCacheClusters</code> • <code>elasticache:DescribeServiceUpdates</code> • <code>elasticfilesystem:DescribeAccessPoints</code> • <code>elasticloadbalancing:DescribeLoadBalancers</code> • <code>elasticloadbalancing:DescribeSslPolicies</code> 	

Modifica	Descrizione	Data
	<ul style="list-style-type: none">• 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
	<ul style="list-style-type: none"> • 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 	
<p>AWSAuditManagerServiceRolePolicy</p> <p>: aggiornamento a una policy esistente</p>	<p>Abbiamo aggiunto la seguenti autorizzazione relativa a <code>AWSAuditManagerServiceRolePolicy</code> :</p> <ul style="list-style-type: none"> • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets 	<p>07/07/2022</p>

Modifica	Descrizione	Data
AWSAuditManagerServiceRolePolicy : aggiornamento a una policy esistente	<p>Il ruolo collegato al servizio ora consente di AWS Audit Manager eseguire l'azione. <code>organizations:DescribeOrganization</code></p> <p>Abbiamo anche suddiviso la risorsa <code>CreateEventsAccess</code> da un carattere jolly (*) a un tipo specifico di risorsa (<code>arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver</code>).</p> <p>Infine, abbiamo aggiunto un operatore di condizione <code>Null</code> per la chiave di condizione <code>events:source</code> per confermare che esiste un valore di origine e che il suo valore non è nullo.</p>	20/05/2022
AWSAuditManagerAdministratorAccess : aggiornamento a una policy esistente	Abbiamo aggiornato la policy delle condizioni chiave per <code>events:source</code> 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 <code>events:source</code> 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 di AWS Audit Manager identità e accesso

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Audit Manager e di IAM.

Argomenti

- [Non sono autorizzato a eseguire alcuna azione in AWS Audit Manager](#)

- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Audit Manager risorse](#)

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 ad Audit Manager.

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 Audit Manager. 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 accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se Audit Manager supporti 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 di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente IAM.

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 Audit Manager. 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. Audit Manager definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo Audit Manager 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 Audit Manager 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, Audit Manager 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:DescribeEndpointConfig`
- `sagemaker:ListEndpointConfigs`
- `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 Audit Manager 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 [Abilita 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 Audit Manager, 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 Audit Manager, 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, Audit Manager non utilizza più il ruolo collegato al servizio.

Per istruzioni su come annullare la registrazione Audit Manager, consulta le seguenti risorse:

- [Disabilita 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 Audit Manager, consulta [Eliminazione dei dati di Audit Manager](#) 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/](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 [GetRole](#) per 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'[DescribeOrganization](#) API 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 tutti i Servizi AWS sono idonei all'HIPAA. Per ulteriori informazioni, consulta la sezione [Riferimenti sui servizi conformi ai requisiti HIPAA](#).

- [AWS Risorse 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 che 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.

Resilienza in AWS Audit Manager

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni 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 su AWS regioni e zone di disponibilità, consulta Global 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 Audit Manager 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 Audit Manager 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 Audit Manager. 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 Audit Manager elencate per tutti i principali su tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "auditmanager:GetAssessments",
        "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 Audit Manager 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

Audit Manager 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 Audit Manager. 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-k112m3n4o5p6"
    ],
  "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-k112m3n4o5p6"
    }
}
```

```
}  
}
```

Prerequisiti per la creazione di una regola EventBridge

Prima di creare regole per gli eventi Audit Manager, 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/](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. Mantieni 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, scegli 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 Audit Manager, 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 Audit Manager 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 Audit Manager e le chiamate di codice alle operazioni delle API Audit Manager.

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 eventi recenti in 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 `CreateCustomControl` operazioni `DeleteControl` e `UpdateAssessmentTemplate` 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 Audit Manager

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"
}
```

Analisi della configurazione e della vulnerabilità in AWS Audit Manager

La configurazione e i controlli IT sono una responsabilità condivisa tra voi AWS e voi, nostri clienti. Per ulteriori informazioni, consulta il [modello di responsabilità AWS condivisa](#).

Tagging delle risorse AWS Audit Manager

Un tag è un'etichetta di metadati assegnata dall'utente o da AWS a 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 `stage` e il valore di una risorsa come `test`.

I tag consentono di:

- Individua facilmente le tue risorse Audit Manager. 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.
- Identificazione e organizzazione delle risorse AWS. Molti Servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate.
- Tenere traccia dei costi AWS. Questi tag vengono attivati nel pannello di controllo AWS Billing and Cost Management. Usa i tag per categorizzare i costi e fornire un report di allocazione dei costi mensili. 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.

Nelle sezioni seguenti vengono fornite ulteriori informazioni sui tag di AWS Audit Manager.

Risorse supportate in Audit Manager

Le seguenti risorse di Audit Manager supportano l'assegnazione dei tag:

- Valutazioni
- Controlli
- Framework

Limitazioni applicate ai tag

Le seguenti restrizioni di base si applicano ai tag sulle risorse di Audit Manager:

- 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; l'utilizzo di questo prefisso è esclusivo di AWS

Gestione dei tag

È possibile impostare i tag come proprietà quando si crea una valutazione, un framework o un controllo. Puoi aggiungere, modificare ed eliminare i 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 le valutazioni:
 - [Creazione di una valutazione](#) e [Modifica di una valutazione](#) nella sezione Valutazioni di questa guida
 - [Scheda Tag](#) nella sezione Rivedi una valutazione di questa guida
 - [CreateAssessment](#) e [UpdateAssessment](#) nell'AWS Audit ManagerAPI Reference
 - [TagResource](#) e [UntagResource](#) nell'AWS Audit ManagerAPI Reference
- Per i framework:
 - [Creazione di un framework personalizzato](#) e [Modifica di un framework personalizzato](#) nella sezione relativa alla libreria Framework di questa guida
 - [Scheda Tag](#) nella sezione Visualizza i dettagli del framework di questa guida
 - [CreateAssessmentFramework](#) e [UpdateAssessmentFramework](#) in Riferimento API AWS Audit Manager
 - [TagResource](#) e [UntagResource](#) in Riferimento API AWS Audit Manager
- Per i controlli:
 - [Creazione di un controllo personalizzato](#) e [Modifica di un controllo personalizzato](#) nella sezione Libreria di controlli di questa guida
 - [Scheda Tag](#) nella sezione Visualizza i dettagli di controllo di questa guida
 - [CreateControl](#) e [UpdateControl](#) nell'AWS Audit ManagerAPI Reference
 - [TagResource](#) e [UntagResource](#) nell'AWS Audit ManagerAPI Reference

Creazione di risorse AWS Audit Manager con AWS CloudFormation

AWS Audit Manager è integrato con AWS CloudFormation, un servizio che ti consente di modellare e configurare le tue risorse AWS in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Puoi creare un modello che descrive tutte le risorse AWS desiderate (ad esempio le tue valutazioni) e AWS CloudFormation si occuperà del provisioning e della configurazione di queste risorse per tuo conto.

Quando usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Audit Manager in modo coerente e continuo. Descrivere le risorse una volta e quindi allestisci le stesse risorse più volte in più regioni e account AWS.

Audit Manager e modelli AWS CloudFormation

Per eseguire l'assegnazione e la configurazione delle risorse per Audit Manager 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 di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a utilizzare 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.

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [Guida per l'utente di AWS CloudFormation](#)
- [Documentazione di riferimento dell'API AWS CloudFormation](#)
- [Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation](#)

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
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato il AWSAuditManagerServiceRolePolicy . Per ulteriori informazioni, consulta la sezione Policy gestite da AWS per AWS Audit Manager .	17 maggio 2024
Politica AWS gestita aggiornata	AWS Audit Manager ha aggiornato la AWSAuditManagerAdministratorAccess politica. Per ulteriori informazioni, consulta la sezione 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 la sezione 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	15 maggio 2024

Chiamate API supportate per origini dati di controllo personalizzate.		
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 la sezione 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 la sezione 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 Audit Manager. 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 tuoi 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 disabiliti Audit Manager. Per ulteriori informazioni, consulta Disabilitazione AWS Audit Manager ed Eliminazione dei dati di Audit Manager .	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 la sezione 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 la sezione 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 AWSAuditManagerAdministratorAccess politica. Per ulteriori informazioni, consulta la sezione 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 e 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 la sezione [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 Audit Manager per monitorare le valutazioni attive e identificare rapidamente le prove non conformi. Per ulteriori informazioni, consulta Utilizzo della dashboard di Audit Manager .	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

Glossario per AWS

Per la terminologia AWS più recente, consultare il [glossario AWS](#) nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.