aws

Guida di amministrazione

Amazon Detective

Amazon Detective: Guida di amministrazione

Table of Contents

Cos'è Amazon Detective?

Amazon Detective consente di analizzare, esaminare e identificare rapidamente la causa principale degli esiti di sicurezza o delle attività sospette. Detective raccoglie automaticamente i dati di log dalle tue risorse AWS. Utilizza quindi il machine learning, l'analisi statistica e la teoria dei grafi per generare visualizzazioni che consentono di condurre indagini sulla sicurezza più rapide ed efficaci. Le aggregazioni di dati, i riepiloghi e il contesto predefiniti di Detective facilitano e velocizzano l'analisi e la determinazione della natura e dell'estensione dei possibili problemi di sicurezza.

Con Detective puoi accedere fino a un anno di dati storici degli eventi. Questi dati sono disponibili attraverso una serie di visualizzazioni che mostrano le variazioni del tipo e del volume di attività in una finestra temporale selezionata. Detective collega queste modifiche ai risultati di GuardDuty. Per ulteriori informazioni sui dati di origine in Detective, consulta Dati di origine utilizzati in un grafico di comportamento.

Come funziona Detective?

Detective estrae automaticamente eventi temporali, ad esempio tentativi di accesso, chiamate API e traffico di rete da AWS CloudTrail e dai log di flusso VPC di Amazon. Inoltre, importa i risultati rilevati da GuardDuty.

A partire da questi eventi, Detective utilizza il machine learning e la visualizzazione per creare una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni tra di esse nel tempo. È possibile esplorare questo grafico del comportamento per esaminare possibili azioni, come i tentativi di accesso non riusciti o le chiamate API sospette. È anche possibile vedere in che modo queste azioni interessano risorse come account AWS e istanze Amazon EC2. Puoi modificare l'ambito e la tempistica del grafico di comportamento per una serie di attività:

- Esamina rapidamente qualsiasi attività che non rientri nella norma.
- Identifica gli schemi che possono indicare un problema di sicurezza.
- Scopri tutte le risorse interessate da un risultato.

Le visualizzazioni personalizzate di Detective forniscono una base e riepilogano le informazioni sull'account. Questi risultati possono aiutare a rispondere a domande come "È una chiamata API insolita per questo ruolo?" Oppure "È previsto questo picco di traffico da questa istanza?"

Con Detective, non è più necessario organizzare i dati o sviluppare, configurare o ottimizzare le query e i propri algoritmi. Non sono previsti costi anticipati, vengono addebitati solo gli eventi analizzati, senza software aggiuntivo da implementare o altri feed a cui abbonarsi.

Chi usa Detective?

Quando un account abilita Detective, diventa l'account amministratore per un grafico di comportamento. Un grafico di comportamento è un insieme collegato di dati estratti e analizzati da uno o più account AWS. Gli account amministratore invitano gli account membri a contribuire con i propri dati al grafico di comportamento dell'account amministratore.

Detective è anche integrato con AWS Organizations. L'account di gestione dell'organizzazione indica un account amministratore di Detective per l'organizzazione. L'account amministratore di Detective abilita gli account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

Per informazioni su come Detective utilizza i dati di origine degli account del grafico comportamentale, consulta Dati di origine utilizzati in un grafico di comportamento.

Per informazioni su come gli account amministratore gestiscono i grafici del comportamento, consulta Gestione degli account. Per informazioni su come gli account membri gestiscono il grafico di comportamento, gli inviti e le iscrizioni, consulta the section called “Per gli account membri: gestione degli inviti e delle iscrizioni”.

L'account amministratore utilizza le analisi e le visualizzazioni generate dal grafico di comportamento per esaminare le risorse AWS e i risultati di GuardDuty. Utilizzando le integrazioni di Detective con GuardDuty e AWS Security Hub, puoi passare da un risultato GuardDuty contenuto in questi servizi direttamente alla console Detective.

Un'indagine di Detective si concentra sull'attività connessa alle risorse AWS coinvolte. Per una panoramica del processo di indagine in Detective, consulta Come viene usato Amazon Detective per le indagini nella Guida per l'utente di Detective.

Termini e concetti di Amazon Detective

I seguenti termini e concetti sono importanti per comprendere Amazon Detective e il relativo funzionamento.

Account amministratore

L'Account AWS che possiede un grafico di comportamento e che utilizza il grafico per le indagini.

L'account amministratore invita gli account membri a contribuire con i propri dati al grafico di comportamento. Per ulteriori informazioni, consulta the section called “Invito degli account membri a un grafico di comportamento”.

Per il grafico di comportamento dell'organizzazione, l'account amministratore è l'account amministratore Detective designato dall'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”. L'account amministratore di Detective abilita qualsiasi account dell'organizzazione come account membro nel grafico di comportamento dell'organizzazione. Per ulteriori informazioni, consulta the section called “Gestione degli account membri dell'organizzazione”.

Gli account amministratore possono anche visualizzare l'utilizzo dei dati per il grafico di comportamento e rimuovere gli account membri dal grafico di comportamento.

Organizzazione autonoma del sistema (ASO)

L'organizzazione titolata a cui è assegnato un sistema autonomo. Questo sistema autonomo è una rete eterogenea o un insieme di reti che utilizzano logiche e policy di routing simili.

Grafico di comportamento

Un insieme collegato di dati generati da dati di origine in entrata che è associato a uno o più Account AWS.

Ogni grafico di comportamento utilizza la stessa struttura di risultati, entità e relazioni.

Account amministratore delegato (AWS Organizations)

In Organizations, l'account amministratore delegato per un servizio è in grado di gestire l'utilizzo di un servizio per l'organizzazione.

In Detective, l'account amministratore di Detective è anche l'account amministratore delegato, a meno che l'account amministratore di Detective non sia l'account di gestione dell'organizzazione. L'account di gestione dell'organizzazione non può essere un account amministratore delegato.

In Detective, è consentita l'autodelega. Un account di gestione dell'organizzazione può delegare il proprio account come amministratore delegato di Detective, ma ciò verrebbe registrato o memorizzato solo nell'ambito di Detective e non delle organizzazioni.

Account amministratore di Detective

Per il grafico del comportamento dell'organizzazione in una Regione, l'account designato dall'account di gestione dell'organizzazione come account amministratore. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”.

Detective consiglia all'account di gestione dell'organizzazione di scegliere un account diverso dal proprio account.

Se l'account non è l'account di gestione dell'organizzazione, l'account amministratore di Detective è anche l'account amministratore delegato di Detective in Organizations.

Dati di origine di Detective

Versioni elaborate e strutturate delle informazioni provenienti dai seguenti tipi di feed:

- Log dai servizi AWS, come log AWS CloudTrail e log di flusso Amazon VPC
- Risultati di GuardDuty

Detective utilizza i dati dell'origine di Detective per compilare il grafico di comportamento. Detective archivia anche copie dei dati di origine di Detective per supportarne l'analisi.

Entità

Un elemento estratto dai dati importati.

Ogni entità ha un tipo, che identifica il tipo di oggetto che rappresenta. Esempi di tipi di entità includono indirizzi IP, istanze Amazon EC2 e utenti AWS.

Le entità possono essere risorse AWS che gestisci o indirizzi IP esterni che hanno interagito con le tue risorse.

Per ogni entità, i dati di origine vengono utilizzati anche per compilare le proprietà dell'entità. I valori delle proprietà possono essere estratti direttamente dai record di origine o aggregati su più record.

Risultato

Un problema di sicurezza rilevato da Amazon GuardDuty.

Gruppo di risultati

Una raccolta di risultati, entità e prove che potrebbero essere correlate allo stesso evento o problema di sicurezza. Detective genera gruppi di risultati basati su un modello di machine learning integrato.

Prova di Detective

Detective identifica ulteriori prove relative a un gruppo di risultati sulla base dei dati del grafico di comportamento raccolti negli ultimi 45 giorni. Questa prova viene presentata come un risultato con il valore di gravità Informativo. Le prove forniscono informazioni di supporto che evidenziano un'attività insolita o un comportamento sconosciuto potenzialmente sospetto se osservati all'interno di un gruppo di risultati. Un esempio di ciò potrebbero essere le geolocalizzazioni appena osservate o le chiamate API osservate nel periodo di validità di un risultato. Al momento, questi risultati sono visualizzabili solo in Detective e non vengono inviati alla Centrale di sicurezza.

Panoramica degli esiti

Una singola pagina che fornisce un riepilogo delle informazioni su un risultato.

Una panoramica dei risultati contiene l'elenco delle entità coinvolte nei risultati. Dall'elenco, è possibile passare al profilo di un'entità.

Una panoramica dei risultati contiene anche un pannello dei dettagli che contiene gli attributi dei risultati.

Entità ad alto volume

Un'entità che ha connessioni da o verso un gran numero di altre entità durante un intervallo di tempo. Ad esempio, un'istanza EC2 potrebbe avere connessioni da milioni di indirizzi IP. Il numero di connessioni supera la soglia che può essere gestita da Detective.

Quando il periodo di validità corrente contiene un intervallo di tempo ad alto volume, Detective avvisa l'utente.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli per entità con volumi elevati nella Guida per l'utente di Amazon Detective.

Indagine

Processo che consiste nell'individuare un'attività sospetta o interessante, determinarne l'ambito, individuarne la sorgente o la causa sottostante e quindi decidere come procedere.

Account membro

Un Account AWS che un account amministratore ha invitato a fornire dati a un grafico comportamentale. Nel grafico del comportamento dell'organizzazione, un account membro può essere un account dell'organizzazione che l'account amministratore di Detective ha abilitato come account membro.

Gli account membri invitati possono rispondere all'invito del grafico di comportamento e rimuovere il proprio account dal grafico. Per ulteriori informazioni, consulta the section called “Per gli account membri: gestione degli inviti e delle iscrizioni”.

Gli account dell'organizzazione non possono modificare la loro appartenenza al grafico di comportamento dell'organizzazione.

Tutti gli account membri possono inoltre visualizzare le informazioni sull'utilizzo del proprio account attraverso i grafici del comportamento a cui contribuiscono con i dati.

Non hanno altro accesso al grafico di comportamento.

Grafico di comportamento dell'organizzazione

Il grafico di comportamento di proprietà dell'account amministratore di Detective. L'account di gestione dell'organizzazione indica un account amministratore di Detective. Per ulteriori informazioni, consulta the section called “Designazione dell'account amministratore di Detective”.

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective controlla se un account dell'organizzazione è un account membro. Gli account dell'organizzazione non possono auto-rimuoversi dal grafico di comportamento dell'organizzazione.

L'account amministratore di Detective può anche invitare altri account al grafico di comportamento dell'organizzazione.

Profilo

Una singola pagina che fornisce una raccolta di visualizzazioni di dati relative all'attività di un'entità.

Per quanto riguarda i risultati, i profili aiutano gli analisti a determinare se il risultato è fonte di reale preoccupazione o falso positivo.

I profili forniscono informazioni a supporto di un'indagine su un risultato o per una ricerca generale di attività sospette.

Pannello del profilo

Una singola visualizzazione su un profilo. Ogni pannello del profilo ha lo scopo di aiutare a rispondere a una o più domande specifiche per assistere un analista in un'indagine.

I pannelli del profilo possono contenere coppie chiave-valore, tabelle, sequenze temporali, grafici a barre o grafici di geolocalizzazione.

Relazione

Attività che si verifica tra singole entità. Le relazioni vengono estratte anche dai dati di origine in entrata.

Analogamente a un'entità, una relazione ha un tipo, che identifica i tipi di entità coinvolte e la direzione della connessione. Un esempio di tipo di relazione è un indirizzo IP che si connette a un'istanza EC2.

Periodo di validità

La finestra temporale utilizzata per definire l'ambito dei dati visualizzati sui profili.

Il periodo di validità predefinito per un risultato riflette la prima e l'ultima volta in cui è stata osservata l'attività sospetta.

Il periodo di validità predefinito per un profilo di entità è pari alle 24 ore precedenti.

Regioni e quote di Amazon Detective

Quando usi Amazon Detective, tieni presente le seguenti quote.

Regioni ed endpoint di Detective

Per visualizzare l'elenco delle Regioni AWS in cui è disponibile Detective, consulta Endpoint del servizio Detective.

Quote di Detective

Detective ha le seguenti quote, che non possono essere configurate.

Risorsa	Quota	Commenti
Numero di account membro	1.200	Il numero di account membri che un account amministratore può aggiungere a un grafico di comportamento.
Volume dei dati del grafico di comportamento: avviso sul volume	9 TB al giorno	Se il volume di dati del grafico di comportamento è superiore a 9 TB al giorno, Detective visualizza un avviso che indica che il grafico di comportamento si sta avvicinando al volume massimo consentito.
Volume di dati del grafico di comportamento: nessun nuovo account	10 TB al giorno	Se il volume di dati del grafico di comportamento supera i 10 TB al giorno, non è possibile aggiungere un nuovo account membro al grafico.
Volume di dati del grafico di comportamento: interromp i l'importazione dei dati nel grafico di comportamento	15 TB al giorno	Se il volume di dati del grafico di comportamento è superiore a 15 TB al giorno, Detective interrompe l'importa zione dei dati nel grafico di comportam ento.

Risorsa	Quota	Commenti
		La quota di 15 TB al giorno riflette sia il normale volume di dati che i picchi. Per riabilitare l'importazione dei dati, è necessario contattare AWS Support.

Internet Explorer 11 non è supportato

Non è possibile utilizzare Detective con Internet Explorer 11.

Configurazione di Amazon Detective

Quando abiliti Amazon Detective, Detective crea un grafico di comportamento specifico per Regione con il tuo account come account amministratore. Inizialmente questo è l'unico account nel grafico di comportamento. L'account amministratore può quindi invitare altri AWS account a contribuire con i propri dati al grafico del comportamento. Per informazioni, consulta Gestione degli account.

L'abilitazione di Detective in una Regione per la prima volta dà inizio anche a una prova gratuita di 30 giorni per il grafico di comportamento. Se l'account disabilita Detective e poi lo abilita di nuovo, non sarà disponibile alcuna prova gratuita. Per informazioni, consulta Informazioni sulla versione di prova gratuita per i grafici di comportamento.

Dopo la prova gratuita, a ogni account indicato nel grafico di comportamento vengono fatturati i dati con cui contribuisce. L'account amministratore può tenere traccia dell'uso e visualizzare il costo totale previsto per un periodo tipico di 30 giorni per l'intero grafico di comportamento. Per ulteriori informazioni, consulta the section called “Utilizzo e costi dell'account amministratore”. Gli account membri possono tenere traccia dell'utilizzo e dei costi previsti per i grafici di comportamento a cui appartengono. Per ulteriori informazioni, consulta the section called “Monitoraggio dell'utilizzo dell'account membro”.

Indice

Prerequisiti e raccomandazioni di Amazon Detective

Per poter abilitare Amazon Detective, assicurati di disporre di un Account AWS.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

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

Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email 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.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root 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.

Creazione di un utente amministratore

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 Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- 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.

È inoltre necessario considerare i seguenti requisiti e raccomandazioni.

AWS Command Line Interface Versione supportata

Per utilizzarlo AWS CLI per eseguire attività di Detective, la versione minima richiesta è 1.16.303.

Allineamento consigliato con e GuardDuty AWS Security Hub

Se sei registrato GuardDuty e AWS Security Hub, ti consigliamo di utilizzare un account amministratore per tali servizi. Se gli account amministratore sono gli stessi per tutti e tre i servizi, i seguenti punti di integrazione funzionano perfettamente.

- Nel GuardDuty nostro Security Hub, quando visualizzi i dettagli di una GuardDuty scoperta, puoi passare dai dettagli del ritrovamento al profilo di ricerca del Detective.
- In Detective, quando indaghi su un GuardDuty ritrovamento, puoi scegliere l'opzione per archiviarlo.

Se disponi di account amministratore diversi per GuardDuty Security Hub, ti consigliamo di allineare gli account amministratore in base al servizio che utilizzi più frequentemente.

- Se lo usi GuardDuty più frequentemente, abilita Detective utilizzando l'account GuardDuty amministratore.

  Se lo utilizzi AWS Organizations per gestire gli account, designa l'account GuardDuty amministratore come account amministratore Detective per l'organizzazione.

- Se usi Centrale di sicurezza più frequentemente, abilita Detective utilizzando l'account amministratore di Centrale di sicurezza.

  Se utilizzi Organizations per gestire gli account, designa l'account amministratore di Centrale di sicurezza come account amministratore di Detective per l'organizzazione.

Se non puoi utilizzare gli stessi account amministratore in tutti i servizi, dopo aver abilitato Detective, puoi facoltativamente creare un ruolo per più account. Questo ruolo consente a un account amministratore di accedere ad altri account.

Per informazioni su come IAM supporta questo tipo di ruolo, consulta Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà nella Guida per l'utente IAM.

Concessione delle autorizzazioni necessarie per Detective

Prima di poter abilitare Detective, devi assicurarti che il tuo principale IAM disponga delle autorizzazioni di Detective richieste. Il principale può essere un utente o un ruolo esistente in uso oppure puoi crearne uno nuovo da utilizzare per Detective.

Quando ti registri ad Amazon Web Services (AWS), il tuo account viene automaticamente registrato per tutti i Servizi AWS, incluso Amazon Detective. Tuttavia, per abilitare e utilizzare Detective è necessario prima impostare le autorizzazioni che consentono l'accesso alla console Amazon Detective e alle operazioni API. Tu o il tuo amministratore potete farlo utilizzando AWS Identity and Access Management (IAM) per allegare la policy `AmazonDetectiveFullAccess` gestita al vostro principale IAM, che concede l'accesso a tutte le azioni del Detective.

Aggiornamento consigliato della frequenza di GuardDuty CloudWatch notifica

Nel GuardDuty, i rilevatori sono configurati con una frequenza di CloudWatch notifica Amazon per segnalare le occorrenze successive di un risultato. Ciò include l'invio di notifiche a Detective.

Per impostazione predefinita, la frequenza è di sei ore. Ciò significa che anche se un risultato si ripete più volte, le nuove ricorrenze non si rifletteranno in Detective se non sei ore dopo.

Per ridurre il tempo necessario a Detective per ricevere questi aggiornamenti, consigliamo GuardDuty all'account amministratore di modificare l'impostazione dei rilevatori a 15 minuti. Tieni presente che la modifica della configurazione non ha alcun effetto sul costo di utilizzo GuardDuty.

Per informazioni sull'impostazione della frequenza di notifica, consulta Monitoring GuardDuty Findings with Amazon CloudWatch Events nella Amazon GuardDuty User Guide.

Abilitazione di Amazon Detective

Quando abiliti Detective, definisci un account amministratore di Detective e inviti altri account a diventare account membri. La relazione amministratore-membro viene stabilita quando un potenziale account membro accetta l'invito. Per maggiori dettagli, consulta Gestione degli account.

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective gestisce l'appartenenza al grafico di comportamento per tutti gli account dell'organizzazione. Per ulteriori informazioni su come viene gestito l'account amministratore di Detective, vedere Designazione dell'account amministratore Detective per un'organizzazione.

Puoi abilitare Detective dalla console Detective, dall'API Detective o dalla AWS Command Line Interface.

Puoi abilitare Detective solo una volta in ogni Regione. Se sei già l'account amministratore di un grafico di comportamento nella Regione, non puoi abilitare nuovamente Detective in quella Regione.

Abilitazione di Detective (console)

Puoi abilitare Amazon Detective dalla AWS Management Console.

Abilitare Detective (console)

1. Accedi alla AWS Management Console. Quindi, apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegliere Iniziare.
3. Nella pagina Abilita Amazon Detective, Align administrator accounts (consigliato) spiega la raccomandazione per allineare gli account amministratore tra Detective e Amazon GuardDuty and. AWS Security Hub Per informazioni, consulta the section called “Allineamento consigliato con e GuardDuty AWS Security Hub”.
4. Il pulsante Collega policy IAM porta direttamente alla console IAM e apre la policy consigliata. Hai la possibilità di collegare la policy consigliata al principale che usi per Detective. Se non disponi delle autorizzazioni per operare nella console IAM, in Autorizzazioni richieste puoi copiare il nome della risorsa Amazon (ARN) della policy da fornire al tuo amministratore IAM. L'amministratore può quindi collegare la policy per tuo conto.

Verifica che la policy IAM richiesta sia in vigore.

5. La sezione Aggiungi tag consente di aggiungere tag al grafico di comportamento.

   Per aggiungere un tag, procedere come segue:

   a. Scegli Aggiungi nuovo tag.
   b. Per Chiave, inserisci il nome del tag.
   c. In Valore, immetti il valore del tag.

   Per rimuovere un tag, seleziona l'opzione Rimuovi per quel tag.
6. Scegli Abilita Amazon Detective.
7. Dopo aver abilitato Detective, puoi invitare gli account membri al tuo grafico di comportamento.

   Per accedere alla pagina di Gestione dell'account, scegli Aggiungi membri adesso. Per informazioni su come invitare gli account membri, consulta the section called “Invito degli account membri a un grafico di comportamento”.

Abilitazione di Detective (Detective API, AWS CLI)

Puoi abilitare Amazon Detective dall'API Detective o dalla AWS Command Line Interface.

Per abilitare Detective (Detective API, AWS CLI)

- API Detective: usa l'operazione `CreateGraph`.
- AWS CLI: alla riga di comando, esegui il comando `create-graph`.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

Il comando seguente abilita Detective e imposta il valore del tag `Department` su `Security`.

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Attivazione di Detective in tutte le regioni (script Python attivo) GitHub

Detective fornisce uno script open source GitHub che esegue le seguenti operazioni:

- Abilita Detective per un account amministratore in un elenco specificato di Regioni
- Aggiunge un elenco fornito di account membri a ciascuno dei grafici di comportamento risultanti
- Invia le e-mail di invito agli account membri
- Accetta automaticamente gli inviti per gli account membri

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. Utilizzo degli script Python di Amazon Detective

Verifica che i dati vengano estratti

Dopo aver abilitato Detective, inizia a inserire ed estrarre i dati dal tuo AWS account nel tuo grafico comportamentale.

Per l'estrazione iniziale, i dati di solito diventano disponibili nel grafico comportamentale entro 2 ore.

Un modo per verificare che Detective stia estraendo dati è cercare valori di esempio nella pagina Cerca di Detective.

Controllare i valori di esempio nella pagina Cerca

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione selezionare Search (Cerca).
3. Dal menu Seleziona tipo, scegli un tipo di elemento.

   La sezione Esempi dai dati contiene un set di identificatori del tipo selezionato presenti nei dati del grafico di comportamento.

   Se riesci a vedere valori di esempio, allora sai che i dati vengono inseriti ed estratti nel tuo grafico di comportamento.

Informazioni sulla versione di prova gratuita per i grafici di comportamento

Amazon Detective offre una prova gratuita di 30 giorni per ogni account in ogni Regione. La prova gratuita per un account inizia la prima volta che si verifica una delle seguenti azioni.

- Un account abilita Detective manualmente e diventa l'account amministratore per un grafico di comportamento.
- Un account è designato come account amministratore di Detective per un'organizzazione in AWS Organizations e ha Detective abilitato per la prima volta.
- Se l'account amministratore di Detective aveva già attivato Detective prima di essere designato, l'account non avvia una nuova prova gratuita di 30 giorni.
- Un account accetta un invito a diventare un account membro in un grafico di comportamento ed è abilitato come account membro.
- Un account dell'organizzazione viene abilitato come account membro dall'account amministratore di Detective.

La prova gratuita dura 30 giorni da quel momento. All'account non viene addebitato alcun dato elaborato durante quel periodo. Al termine del periodo di prova, Detective inizia a fatturare all'account i dati con cui contribuisce ai grafici di comportamento. Per ulteriori informazioni su come tenere traccia dell'attività di Detective, monitorare l'utilizzo e visualizzare i costi previsti, consulta Monitoraggio delle azioni e dell'utilizzo in Amazon Detective. Per ulteriori informazioni sui prezzi, consulta Prezzi di Detective.

Lo stesso periodo di 30 giorni viene utilizzato per tutti i grafici di comportamento della Regione. Ad esempio, un account è abilitato come account membro per un grafico di comportamento. Inizia la prova gratuita di 30 giorni. Dopo 10 giorni, l'account viene abilitato per un secondo grafico di comportamento nella stessa Regione. Per il secondo grafico di comportamento, l'account riceve 20 giorni di dati gratuiti.

La versione di prova gratuita offre diversi vantaggi:

- Gli account amministratore possono esplorare le caratteristiche e le funzionalità di Detective per verificarne il valore.

- Gli account amministratore e gli account membri possono monitorare la quantità di dati e il costo stimato prima che Detective inizi a fatturarli. Consultare the section called “Utilizzo e costi dell'account amministratore” e the section called “Monitoraggio dell'utilizzo dell'account membro”.

Versione di prova gratuita per origini dati facoltative

Detective offre una prova gratuita di 30 giorni anche per le origini dati facoltative. Questa versione di prova gratuita è separata dalla versione di prova gratuita fornita per le origini dati principali di Detective quando Detective viene abilitato per la prima volta.

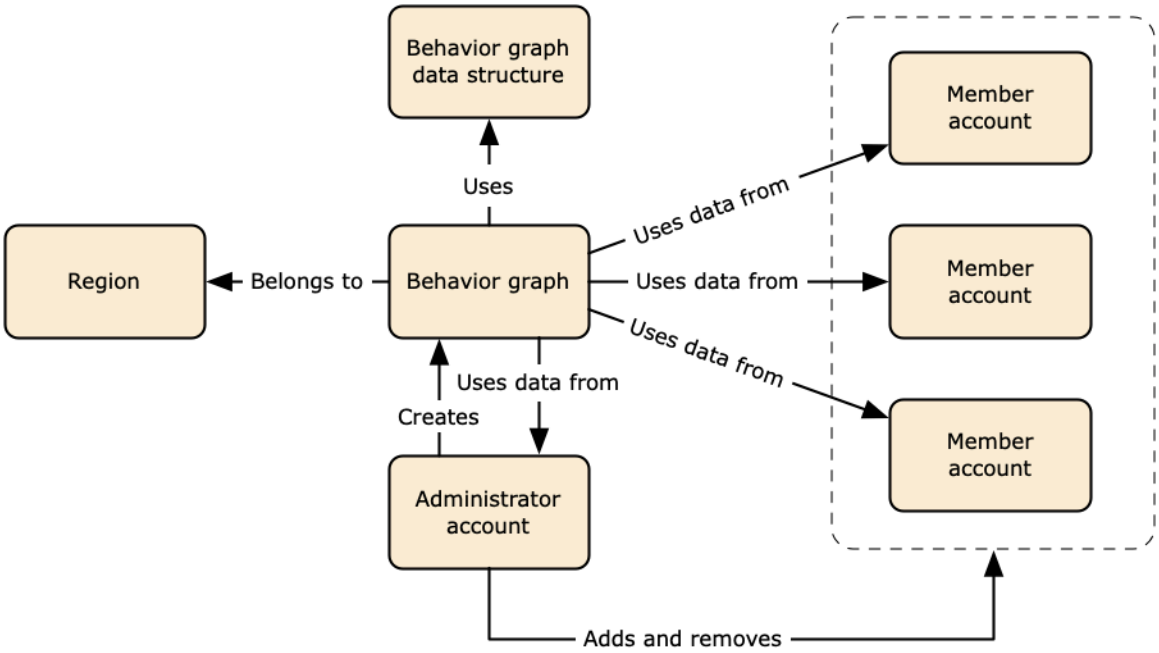
> **Note**
>
> Se un cliente disabilita un pacchetto di origini dati opzionale entro 7 giorni dall'abilitazione, Detective esegue un ripristino automatico una tantum della versione di prova gratuita per quel pacchetto di origini dati, se viene nuovamente abilitato.

Per abilitare o disabilitare un'origine dati facoltativa, consulta Tipi di origini dati facoltativi in Detective.

Dati di origine utilizzati in un grafico di comportamento

Per compilare un grafico di comportamento, Amazon Detective utilizza i dati di origine dell'account amministratore e degli account dei membri del grafico di comportamento.

Con Detective puoi accedere fino a un anno di dati storici degli eventi. Questi dati sono disponibili attraverso una serie di visualizzazioni che mostrano le variazioni del tipo e del volume di attività in una finestra temporale selezionata. Detective collega queste modifiche ai risultati di GuardDuty.



Per i dettagli sulla struttura dei dati del grafico di comportamento, consulta Panoramica della struttura dei dati del grafico di comportamento nella Guida per l'utente di Detective.

Tipi di origini dati principali in Detective

Detective importa i dati dai seguenti tipi di log AWS:

- Log AWS CloudTrail
- Log di flusso Amazon Virtual Private Cloud (Amazon VPC)
- Per gli account registrati a GuardDuty, Detective importa anche i risultati di GuardDuty.

Detective utilizza gli eventi dei log di flusso CloudTrail e VPC utilizzando flussi indipendenti e duplicativi di log di flusso CloudTrail e VPC. Questi processi non influiscono né utilizzano le

configurazioni dei log di flusso CloudTrail e VPC esistenti. Inoltre, non influiscono sulle prestazioni né aumentano i costi di questi servizi.

Tipi di origini dati facoltativi in Detective

Detective offre pacchetti di origini facoltative oltre alle tre origini dati offerte nel pacchetto principale Detective (il pacchetto principale include log AWS CloudTrail, log di flusso VPC e risultati GuardDuty). Un pacchetto di origini dati facoltativo può essere avviato o interrotto per un grafico di comportamento in qualsiasi momento.

Detective offre una prova gratuita di 30 giorni per tutti i pacchetti di origini principali e facoltativi per Regione.

> **Note**
>
> Detective conserva tutti i dati ricevuti da ciascun pacchetto di origini dati per un massimo di 1 anno.

Attualmente sono disponibili i seguenti pacchetti di origini facoltative:

- Log di controllo EKS

  Questo pacchetto di origini dati facoltativi consente a Detective di importare informazioni dettagliate sui cluster EKS nel tuo ambiente e di aggiungere tali dati al grafico di comportamento. Per informazioni dettagliate, consulta Log di controllo di Amazon EKS per Detective.

- Risultati di sicurezza AWS

  Questo pacchetto di origini dati facoltativi consente a Detective di importare dati da Centrale di sicurezza e di aggiungerli al grafico di comportamento. Per informazioni dettagliate, consulta Risultati di sicurezza AWS.

Avvio o arresto di un'origine dati facoltativa:

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.

3. In Pacchetti sorgente opzionali, seleziona Aggiorna. Quindi seleziona l'origine dati che desideri abilitare o deseleziona una casella per un'origine dati già abilitata e scegli Aggiorna per modificare i pacchetti di origini dati abilitati.

> **Note**
>
> Se arresti e poi riavvii un'origine dati facoltativa, vedrai una lacuna nei dati visualizzati su alcuni profili di entità. Questa lacuna verrà rilevata sul display della console e rappresenterà il periodo di tempo in cui l'origine dati è stata arrestata. Quando un'origine dati viene riavviata, Detective non importa i dati in modo retroattivo.

Log di controllo di Amazon EKS per Detective

I log di audit di Amazon EKS sono un pacchetto di origini dati opzionale che può essere aggiunto al grafico di comportamento di Detective. Puoi visualizzare i pacchetti di origine facoltativi disponibili e il rispettivo stato dal tuo account dalla pagina Impostazioni della console o dall'API Detective.

È disponibile una prova gratuita di 30 giorni per questa origini dati. Per ulteriori informazioni, consulta Versione di prova gratuita per origini dati facoltative.

L'abilitazione dei log di controllo di Amazon EKS consente a Detective di aggiungere informazioni approfondite sulle risorse create con Amazon EKS al tuo grafico di comportamento. Questa origine dati migliora le informazioni fornite sui seguenti tipi di entità: cluster EKS, pod Kubernetes, immagine di container e soggetti Kubernetes.

Inoltre, se hai abilitato i log di controllo EKS come origine dati in Amazon GuardDuty, potrai visualizzare i dettagli dei risultati di Kubernetes da GuardDuty. Per ulteriori informazioni sull'abilitazione di questa origine dati in GuardDuty, consulta Protezione di Kubernetes in Amazon GuardDuty.

> **Note**
>
> Questa origine dati è abilitata per impostazione predefinita per i nuovi grafici di comportamento creati dopo il 26 luglio 2022. Per i grafici di comportamento creati prima del 26 luglio 2022, deve essere abilitata manualmente.

Aggiunta o rimozione dei log di controllo di Amazon EKS come origine dati facoltativa:

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.
3. In Pacchetti sorgente, seleziona Log di controllo EKS per abilitare questa origine dati. Se è già abilitata, selezionala nuovamente per interrompere l'importazione dei log di controllo EKS nel tuo grafico di comportamento.

Risultati di sicurezza AWS

I risultati di sicurezza di AWS sono un pacchetto di origini dati facoltativo che può essere aggiunto al grafico di comportamento di Detective.

Puoi visualizzare i pacchetti di origine facoltativi disponibili e il rispettivo stato dal tuo account dalla pagina Impostazioni della console o dall'API Detective.

È disponibile una prova gratuita di 30 giorni per questa origini dati. Per ulteriori informazioni, consulta Versione di prova gratuita per origini dati facoltative.

L'abilitazione dei risultati di sicurezza di AWS consente a Detective di utilizzare i risultati di Centrale di sicurezza aggregati da Centrale di sicurezza dai servizi upstream in un formato di risultati standard chiamato AWS Security Format (ASFF), che elimina la necessità di lunghe conversioni dei dati. Quindi, correla i risultati acquisiti tra i prodotti per definire la priorità di quelli più importanti.

Aggiunta o rimozione dei risultati di sicurezza di AWS come origine dati facoltativa:

> **Note**
>
> L'origine dati dei risultati di sicurezza di AWS è abilitata per impostazione predefinita per i nuovi grafici del comportamento creati dopo il 16 maggio 2023. Per i grafici del comportamento creati prima del 16 maggio 2023, deve essere abilitata manualmente.

1. Apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Generale.
3. In Pacchetti sorgente, seleziona i risultati di sicurezza di AWS per abilitare questa origine dati. Se è già abilitata, selezionala nuovamente per interrompere l'importazione dei risultati di AWS Security Finding Format (ASFF) nel tuo grafico di comportamento.

Risultati correntemente supportati

Detective importa tutti i risultati ASFF in Centrale di sicurezza da servizi di proprietà di Amazon o AWS.

- Per visualizzare l'elenco delle integrazioni di servizi supportate, consulta Integrazioni dei servizi AWS disponibili nella Guida per l'utente di AWS Security Hub.
- Per l'elenco delle risorse supportate, consulta Risorse nella Guida per l'utente di AWS Security Hub.
- I risultati dei servizi AWS con uno stato di conformità non impostato su `FAILED` e i risultati aggregati tra le Regioni non vengono importati.

Come Detective importa e archivia i dati di origine

Quando Detective è abilitato, Detective inizia a importare i dati di origine dall'account amministratore del grafico di comportamento. Man mano che gli account dei membri vengono aggiunti al grafico di comportamento, Detective inizia anche a utilizzare i dati di tali account membro.

I dati di origine di Detective sono costituiti da versioni strutturate ed elaborate dei feed originali. Per supportare l'analisi dei dati di Detective, archivia anche copie dei dati di origine di Detective.

Il processo di importazione di Detective inserisce i dati nei bucket Amazon Simple Storage Service (Amazon S3) dal datastore di origine di Detective. Con l'arrivo di nuovi dati di origine, altri componenti di Detective raccolgono i dati e avviano i processi di estrazione e analisi. Per ulteriori informazioni, consulta Come Detective utilizza i dati di origine per compilare un grafico di comportamento nella Guida per l'utente di Detective.

Come Detective applica la quota di volume di dati per i grafici del comportamento

Detective ha quote rigorose sul volume di dati che consente in ogni grafico di comportamento. Il volume di dati è la quantità di dati al giorno che confluisce nel grafico di comportamento di Detective.

Detective applica queste quote quando un account amministratore abilita Detective e quando un account membro accetta un invito a contribuire a un grafico di comportamento.

- Se il volume di dati per un account amministratore supera i 10 TB al giorno, l'account amministratore non può abilitare Detective.

- Se il volume di dati aggiunto proveniente da un account membro fa sì che il grafico di comportamento superi i 10 TB al giorno, l'account membro non può essere abilitato.

Il volume di dati per un grafico di comportamento può inoltre crescere naturalmente nel tempo. Detective controlla ogni giorno il volume dei dati del grafico di comportamento per assicurarsi che non superi la quota.

Se il volume di dati del grafico di comportamento si avvicina alla quota, Detective visualizza un messaggio di avviso sulla console. Per evitare di superare la quota, è possibile rimuovere gli account membri.

Se il volume di dati del grafico di comportamento supera i 10 TB al giorno, non è possibile aggiungere un nuovo account membro al grafico di comportamento.

Se il volume di dati del grafico di comportamento supera i 15 TB al giorno, Detective interrompe l'importazione dei dati nel grafico di comportamento. La quota di 15 TB al giorno riflette sia il normale volume di dati che i picchi del volume di dati. Quando viene raggiunta questa quota, non vengono inseriti nuovi dati nel grafico di comportamento, ma i dati esistenti non vengono rimossi. È comunque possibile utilizzare tali dati storici per le indagini. La console visualizza un messaggio per indicare che l'importazione dei dati è sospesa per il grafico di comportamento.

Se l'importazione dei dati è sospesa, è necessario utilizzare AWS Support per riabilitarla. Se possibile, prima di contattare AWS Support, prova a rimuovere gli account membri per portare il volume di dati al di sotto della quota. Ciò semplifica la riabilitazione dell'importazione dei dati per il grafico di comportamento.

Gestione degli account

Ogni grafico di comportamento contiene i dati di uno o più account. Quando un account abilita Detective, diventa l'account amministratore per il grafico di comportamento e sceglie gli account membri per il grafico. Un grafico di comportamento può contenere fino a 1.200 account membri.

Se sei integrato con AWS Organizations, l'account di gestione dell'organizzazione designa l'account amministratore Detective per l'organizzazione. Quell'account amministratore di Detective diventa quindi l'account amministratore per il grafico di comportamento dell'organizzazione. L'account amministratore di Detective abilita qualsiasi account dell'organizzazione come account membro nel grafico di comportamento dell'organizzazione. Gli account dell'organizzazione non possono rimuoversi dal grafico di comportamento dell'organizzazione.

Un account amministratore può invitare gli account a contribuire con i propri dati a un grafico di comportamento. Quando l'account accetta l'invito, Detective abilita l'account come account membro. Gli account membri aggiunti su invito possono rimuovere se stessi dal grafico di comportamento.

Quando un account viene abilitato come account membro, Detective inizia a importare ed estrarre i dati dell'account membro in quel grafico di comportamento.

Amazon Detective addebita a ciascun account i dati con cui contribuisce per ogni grafico di comportamento. Per informazioni sul monitoraggio del volume di dati per ciascun account in un grafico di comportamento, consulta the section called “Utilizzo e costi dell'account amministratore”.

Indice

Restrizioni e raccomandazioni sugli account in Detective

Quando gestisci gli account di Amazon Detective, considera le seguenti restrizioni e raccomandazioni.

Numero massimo di account membri

Detective consente fino a 1.200 account membri in ogni grafico di comportamento.

Account e Regioni

Se utilizzi AWS Organizations per gestire gli account, l'account di gestione dell'organizzazione designa un account amministratore di Detective per l'organizzazione. L'account amministratore di Detective diventa l'account amministratore per il grafico di comportamento dell'organizzazione.

L'account amministratore di Detective deve essere lo stesso in tutte le Regioni. L'account di gestione dell'organizzazione designa l'account amministratore di Detective separatamente in ciascuna Regione. L'account amministratore di Detective gestisce anche i grafici del comportamento dell'organizzazione e gli account membri separatamente in ciascuna Regione.

Per gli account membro creati per invito, l'associazione amministratore-membro viene creata solo nella Regione da cui viene inviato l'invito. L'account amministratore deve abilitare Detective in ogni Regione e dispone di un grafico del comportamento separato in ogni Regione. L'account amministratore invita quindi ogni account ad associarsi come account membro in quella Regione.

Un account può essere un account membro di più grafici del comportamento nella stessa Regione. Un account può essere solo l'account amministratore di un grafico del comportamento per Regione. Un account può essere un account amministratore in diverse Regioni.

Allineamento degli account amministratori con Centrale di sicurezza e GuardDuty

Per garantire il corretto funzionamento delle integrazioni con AWS Security Hub e Amazon GuardDuty, consigliamo di utilizzare lo stesso account come account amministratore in tutti questi servizi.

Per informazioni, consultare the section called “Allineamento consigliato con e GuardDuty AWS Security Hub”.

Concessione delle autorizzazioni necessarie per gli account amministratore

Per garantire che un account amministratore disponga delle autorizzazioni necessarie per gestire il relativo grafico del comportamento, collega la policy gestita `AmazonDetectiveFullAccess` al principale IAM.

Riflesso degli aggiornamenti dell'organizzazione in Detective

Le modifiche a un'organizzazione non si riflettono immediatamente in Detective.

Per la maggior parte delle modifiche, ad esempio account dell'organizzazione nuovi e rimossi, perché Detective riceva una notifica potrebbe essere necessaria fino a un'ora.

La propagazione di una modifica all'account amministratore Detective designato in Organizations richiede meno tempo.

Transizione all'utilizzo di Organizations per gestire gli account dei grafici di comportamento

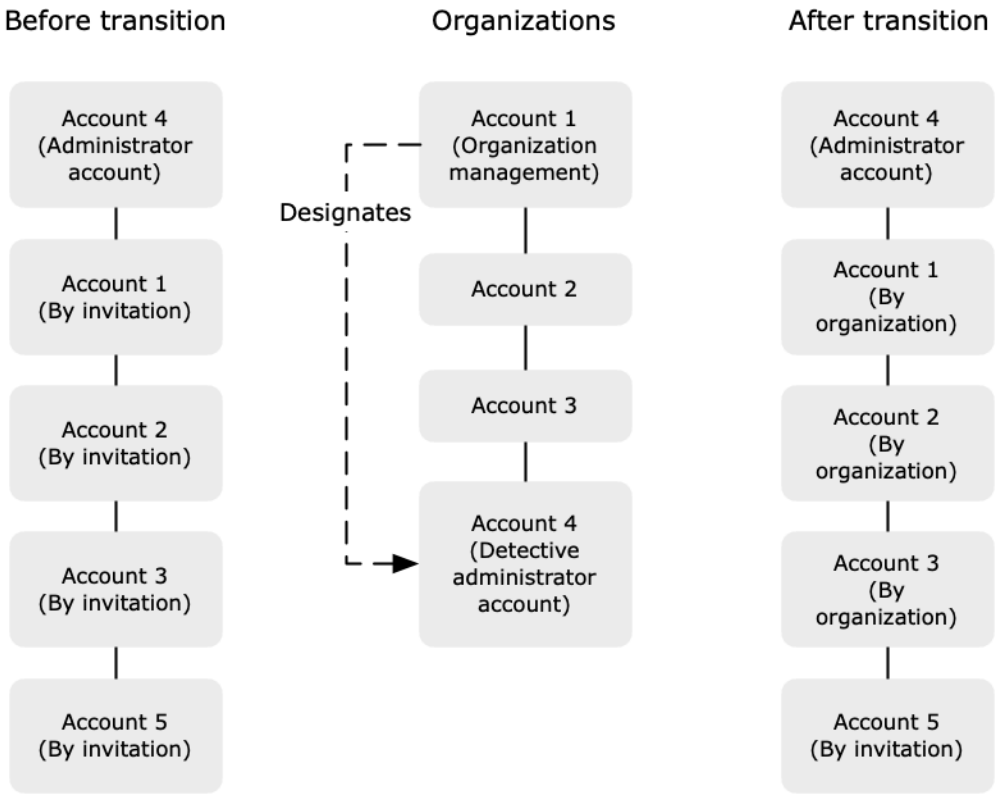
Potresti avere già un grafico di comportamento con gli account membri che hanno accettato un invito manuale. Se sei registrato a AWS Organizations, completa la procedura seguente per utilizzare Organizations per abilitare e gestire gli account membri invece di utilizzare la procedura di invito manuale:

1. Designa l'account amministratore di Detective per l'organizzazione. Questo crea il grafico di comportamento dell'organizzazione.

   Se l'account amministratore di Detective ha già un grafico di comportamento, quel grafico diventa il grafico di comportamento dell'organizzazione.
2. Abilita gli account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

   Se il grafico di comportamento dell'organizzazione dispone di account membri esistenti che sono account dell'organizzazione, tali account vengono abilitati automaticamente.

Il diagramma seguente mostra una panoramica della struttura del grafico di comportamento prima della transizione, la configurazione in Organizations e la struttura degli account del grafico di comportamento dopo la transizione.



Designa un account amministratore di Detective per l'organizzazione.

L'account di gestione dell'organizzazione designa un account amministratore di Detective dalla tua organizzazione. Per informazioni, consultare the section called “Designazione dell'account amministratore di Detective”.

Per semplificare la transizione, Detective consiglia di scegliere un account amministratore corrente come account amministratore di Detective per l'organizzazione.

Se esiste un account amministratore delegato per Detective in Organizations, è necessario utilizzare tale account o l'account di gestione dell'organizzazione come account amministratore di Detective.

Altrimenti, la prima volta che si designa un account amministratore di Detective diverso dall'account di gestione dell'organizzazione, Detective chiama Organizations per rendere quell'account l'account amministratore delegato di Detective.

Abilitare gli account dell'organizzazione come account membri

L'account amministratore di Detective è l'account amministratore per il grafico di comportamento dell'organizzazione. L'account amministratore di Detective sceglie gli account dell'organizzazione da

abilitare come account membri nel grafico di comportamento dell'organizzazione. Per informazioni, consultare the section called “Gestione degli account membri dell'organizzazione”.

Nella pagina Account, l'account amministratore di Detective visualizza tutti gli account dell'organizzazione.

Se l'account amministratore di Detective era già l'account amministratore per un grafico di comportamento, quel grafico diventa il grafico di comportamento dell'organizzazione. Gli account dell'organizzazione che erano già account membri nel grafico di comportamento vengono abilitati automaticamente come account membro. Lo stato degli altri account dell'organizzazione è Non membro.

Gli account dell'organizzazione hanno il tipo Per organizzazione, anche se in precedenza erano account membri per invito.

Gli account membri che non appartengono all'organizzazione hanno il tipo Per invito.

La pagina Gestione dell'account fornisce anche un'opzione, Abilita automaticamente i nuovi account dell'organizzazione, per abilitare automaticamente i nuovi account man mano che vengono aggiunti a un'organizzazione. Per informazioni, consultare the section called “Abilitazione automatica di nuovi account dell'organizzazione”. L'opzione è inizialmente disattivata.

Quando l'account amministratore di Detective visualizza per la prima volta la pagina Gestione dell'account, viene visualizzato un messaggio che contiene il pulsante Abilita tutti gli account dell'organizzazione. Quando scegli Abilita tutti gli account dell'organizzazione, Detective completa le seguenti operazioni:

- Abilita tutti gli account dell'organizzazione correnti come account membri.
- Attiva l'opzione per abilitare automaticamente nuovi account dell'organizzazione.

Nell'elenco degli account membri è disponibile anche l'opzione Abilita tutti gli account dell'organizzazione.

Operazioni disponibili per gli account

Gli account amministratore e gli account membri hanno accesso alle seguenti operazioni di Detective. Nella tabella, i valori hanno i seguenti significati:

- Qualsiasi: l'account può eseguire l'operazione per tutti gli account dello stesso account amministratore di Detective.

- Personale: l'account può eseguire l'operazione solo sul proprio account.
- Trattino (–): l'account non può eseguire l'operazione.

La tabella seguente riporta le autorizzazioni predefinite per gli account amministratore e membro. È possibile utilizzare policy IAM personalizzate per limitare ulteriormente l'accesso alle caratteristiche e alle funzionalità di Detective.

Azione	Account amministratore (organizzazione)	Account amministratore (invito)	Membro (organizzazione)	Membro (invito)
Visualizzazione degli account	Qualsiasi	Qualsiasi	Personale (visualizza gli account amministratori)	Personale (visualizza gli account amministratori)
Rimozione di un account membro	Qualsiasi Gli account invitati vengono rimossi Gli account dell'orga nizzazione sono dissociati	Qualsiasi	–	Personale
Aggiunta o rimozione dei pacchetti di origini dati facoltative	Qualsiasi (l'impostazione si applica a tutti gli account membri)	Qualsiasi (l'impostazione si applica a tutti gli account membri)	–	–
Disabilitazione di Detective	Personale	Personale	–	–
Visualizz azione dei dati	Qualsiasi	Qualsiasi	–	–

Azione	Account amministratore (organizzazione)	Account amministratore (invito)	Membro (organizzazione)	Membro (invito)
del grafico di comportamento				
Abilitazione o disabilitazione dei pacchetti di origini dati facoltative	Tutti	Tutti	–	–

Designazione dell'account amministratore di Detective per un'organizzazione

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective gestisce l'appartenenza al grafico di comportamento per tutti gli account dell'organizzazione.

Come viene gestito l'account amministratore di Detective

L'account di gestione dell'organizzazione designa un account amministratore di Detective per l'organizzazione in ogni Regione AWS.

Impostazione dell'account amministratore di Detective come account amministratore delegato

L'account amministratore di Detective diventa anche l'account amministratore delegato per Detective in AWS Organizations. L'eccezione è se l'account di gestione dell'organizzazione designa se stesso come account amministratore di Detective. L'account di gestione dell'organizzazione non può essere un amministratore delegato in Organizations.

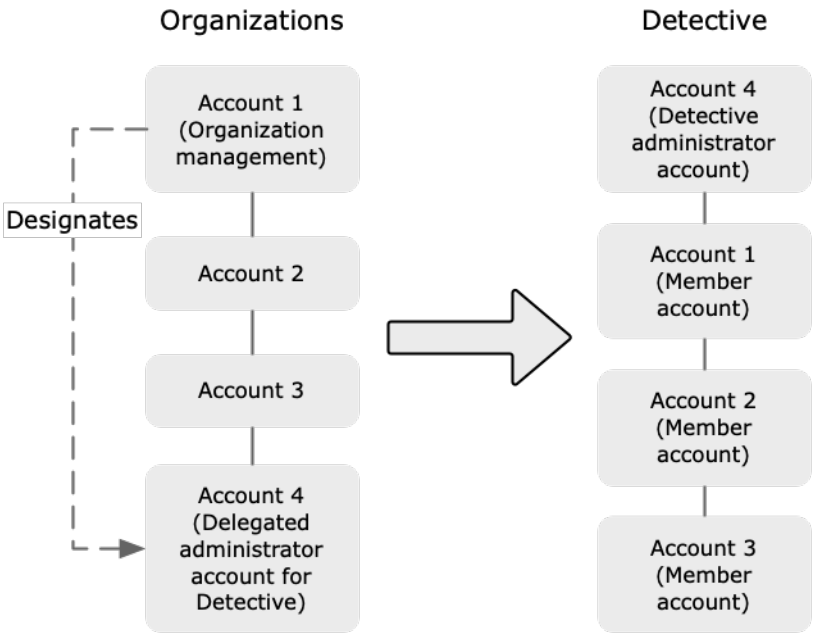
Dopo aver impostato l'account amministratore delegato in Organizations, l'account di gestione dell'organizzazione può scegliere solo l'account amministratore delegato o il proprio account come account amministratore di Detective. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.

Creazione e gestione del grafico di comportamento dell'organizzazione

Quando l'account di gestione dell'organizzazione sceglie un account amministratore di Detective, Detective crea un nuovo grafico di comportamento per quell'account. Questo grafico di comportamento è il grafico di comportamento dell'organizzazione.

Se l'account amministratore di Detective è un account amministratore per un grafico di comportamento esistente, quel grafico di comportamento diventa il grafico di comportamento dell'organizzazione.

L'account amministratore di Detective sceglie gli account dell'organizzazione da abilitare come account membri nel grafico di comportamento dell'organizzazione.



L'account amministratore di Detective può anche inviare inviti agli account che non appartengono all'organizzazione. Per ulteriori informazioni, consulta the section called “Gestione degli account membri dell'organizzazione” e the section called “Gestione degli account invitati”.

Rimozione dell'account amministratore di Detective

L'account di gestione dell'organizzazione può rimuovere l'account amministratore di Detective corrente in una Regione. Quando rimuovi l'account amministratore di Detective, Detective lo rimuove solo dalla Regione corrente. Non modifica l'account amministratore delegato in Organizations.

Quando l'account di gestione dell'organizzazione rimuove l'account amministratore di Detective in una Regione, Detective elimina il grafico di comportamento dell'organizzazione. Detective è disabilitato per l'account amministratore di Detective rimosso.

Per rimuovere l'account amministratore delegato corrente per Detective, puoi utilizzare l'API Organizations. Quando si rimuove l'account amministratore delegato per Detective in Organizations, Detective elimina tutti i grafici di comportamento dell'organizzazione in cui l'account amministratore delegato è l'account amministratore di Detective. I grafici di comportamento dell'organizzazione che hanno l'account di gestione dell'organizzazione come account amministratore di Detective non sono interessati.

Autorizzazioni richieste per configurare l'account amministratore di Detective

Per garantire che l'account di gestione dell'organizzazione sia in grado di configurare l'account amministratore di Detective, puoi allegare la policy gestita `AmazonDetectiveOrganizationsAccess` alle tue entità AWS Identity and Access Management (IAM).

Designazione di un account amministratore di Detective (console)

L'account di gestione dell'organizzazione può utilizzare la console Detective per designare l'account amministratore di Detective.

Non è necessario abilitare Detective per gestire l'account amministratore di Detective. Puoi gestire l'account amministratore di Detective dalla pagina Abilita Detective.

Designare un account amministratore di Detective (pagina Abilita Detective)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegli Inizia.
3. Nel pannello Autorizzazioni richieste per gli account amministratore, concedi le autorizzazioni necessarie all'account che scegli in modo che possa funzionare come amministratore di Detective con accesso completo a tutte le operazioni in Detective. Per operare come amministratore, consigliamo di allegare la policy `AmazonDetectiveFullAccess` al principale.
4. Scegli Collega policy da IAM per visualizzare la policy consigliata direttamente nella console IAM.
5. A seconda che tu disponga delle autorizzazioni nella console IAM, procedi come segue:

- Se disponi delle autorizzazioni per operare nella console IAM, collega la policy consigliata al principale che usi per Detective.
- Se non disponi delle autorizzazioni per operare nella console IAM, copia il nome della risorsa Amazon (ARN) della policy e forniscilo al tuo amministratore IAM. Possono quindi allegare la policy per tuo conto.

6. In Amministratore delegato, scegli l'account amministratore di Detective.

   Le opzioni disponibili dipendono dal fatto se si dispone di un account amministratore delegato per Detective in Organizations.

   - Se non disponi di un account amministratore delegato per Detective in Organizations, inserisci l'identificatore dell'account per designarlo come account amministratore di Detective.

     Potresti avere già un account amministratore e un grafico di comportamento ottenuti dalla procedura di invito manuale. In tal caso, consigliamo di designare quell'account come account amministratore di Detective.

     Se disponi di un account amministratore delegato in Organizations for Amazon GuardDuty, AWS Security Hub o Amazon Macie, Detective ti chiederà di selezionare uno di questi account. Puoi anche inserire un account diverso.
   - Se disponi di un account amministratore delegato per Detective in Organizations, ti verrà richiesto di scegliere quell'account o il tuo account. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.

7. Scegli Delega.

Se hai abilitato Detective o sei un account membro in un grafico di comportamento esistente, allora puoi designare l'account amministratore di Detective dalla pagina Generale.

Designare un account amministratore di Detective (pagina Generale)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.
3. Nel pannello Policy gestite, puoi saperne di più su tutte le policy gestite supportate da Detective. Puoi concedere le autorizzazioni necessarie a un account a seconda delle operazioni che desideri che gli utenti eseguano in Detective. Per operare come amministratore, consigliamo di allegare la policy `AmazonDetectiveFullAccess` al principale.

4. A seconda che tu disponga delle autorizzazioni nella console IAM, procedi come segue:

   - Se disponi delle autorizzazioni per operare nella console IAM, collega la policy consigliata al principale che usi per Detective.
   - Se non disponi delle autorizzazioni per operare nella console IAM, copia il nome della risorsa Amazon (ARN) della policy e forniscilo al tuo amministratore IAM. Possono quindi allegare la policy per tuo conto.

   Le opzioni disponibili dipendono dal fatto se si dispone di un account amministratore delegato per Detective in Organizations.

   - Se non disponi di un account amministratore delegato per Detective in Organizations, inserisci l'identificatore dell'account per designarlo come account amministratore di Detective.

     Potresti avere già un account amministratore e un grafico di comportamento ottenuti dalla procedura di invito manuale. In tal caso, ti consigliamo di designare quell'account come account amministratore di Detective.

     Se disponi di un account amministratore delegato in Organizations for Amazon GuardDuty, AWS Security Hub o Amazon Macie, Detective ti chiederà di selezionare uno di questi account. Puoi anche inserire un account diverso.
   - Se disponi di un account amministratore delegato per Detective in Organizations, ti verrà richiesto di scegliere quell'account o il tuo account. Ti consigliamo di scegliere l'account amministratore delegato in tutte le Regioni.
5. Scegli Delega.

Designazione di un account amministratore di Detective (API Detective, AWS CLI)

Per designare l'account amministratore di Detective, puoi utilizzare una chiamata API o la AWS Command Line Interface. È necessario utilizzare le credenziali dell'account di gestione della tua organizzazione.

Se disponi già di un account amministratore delegato per Detective nelle organizzazioni, devi scegliere quell'account o il tuo account; ti consigliamo di scegliere l'account amministratore delegato.

Designare l'account amministratore di Detective (API Detective, AWS CLI)

- API Detective: usa l'operazione `EnableOrganizationAdminAccount`. È necessario fornire l'identificativo dell'account AWS dell'account amministratore di Detective. Per ottenere l'identificatore dell'account, utilizza l'operazione `ListOrganizationAdminAccounts`.
- AWS CLI: alla riga di comando, esegui il comando `enable-organization-admin-account`.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Esempio

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Rimozione di un account amministratore di Detective (console)

Dalla console Detective, è possibile rimuovere l'account amministratore di Detective.

Quando rimuovi l'account amministratore di Detective, Detective viene disabilitato per l'account e il grafico di comportamento dell'organizzazione viene eliminato. L'account amministratore di Detective viene rimosso solo nella regione corrente.

> **Important**
>
> La rimozione di un account amministratore di Detective non influisce sull'account amministratore delegato in Organizations.

Rimuovere l'account amministratore di Detective (pagina Abilita Detective)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Scegli Inizia.
3. In Amministratore delegato, scegli Disabilita Amazon Detective.
4. Nella finestra di dialogo di conferma, inserisci **`disable`** e quindi seleziona Disabilita Amazon Detective.

Rimuovere un account amministratore di Detective (pagina Generale)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.
3. In Amministratore delegato, scegli Disabilita Amazon Detective.
4. Nella finestra di dialogo di conferma, inserisci **`disable`** e quindi seleziona Disabilita Amazon Detective.

Rimozione dell'account amministratore di Detective (API Detective, AWS CLI)

Per designare l'account amministratore di Detective, puoi utilizzare una chiamata API o la AWS CLI. È necessario utilizzare le credenziali dell'account di gestione della tua organizzazione.

Quando rimuovi l'account amministratore di Detective, Detective viene disabilitato per l'account e il grafico di comportamento dell'organizzazione viene eliminato.

> **Important**
>
> La rimozione di un account amministratore di Detective non influisce sull'account amministratore delegato in Organizations.

Rimuovere l'account amministratore di Detective (API Detective, AWS CLI)

- API Detective: usa l'operazione `DisableOrganizationAdminAccount`.

  Quando si utilizza l'API Detective per rimuovere l'account amministratore di Detective, questo viene rimosso solo nella Regione in cui è stata emessa la chiamata API o il comando.
- AWS CLI: alla riga di comando, esegui il comando `disable-organization-admin-account`.

```
aws detective disable-organization-admin-account
```

Rimozione dell'account amministratore delegato (API Organizations, AWS CLI)

La rimozione dell'account amministratore di Detective non rimuove automaticamente l'account amministratore delegato in Organizations. Per rimuovere l'account amministratore di Detective, puoi utilizzare l'API Organizations.

Quando si rimuove l'account amministratore delegato, vengono eliminati tutti i grafici di comportamento dell'organizzazione in cui l'account amministratore delegato è l'account amministratore di Detective. Disabilita inoltre Detective per l'account in quelle Regioni.

Rimuovere l'account amministratore delegato (API Organizations, AWS CLI)

- API Organizations: utilizza l'operazione `DeregisterDelegatedAdministrator`. È necessario fornire l'identificatore dell'account amministratore di Detective e il principale di servizio per Detective, ovvero `detective.amazonaws.com`.
- AWS CLI: alla riga di comando, esegui il comando `deregister-delegated-administrator`.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Esempio

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Visualizzazione dell'elenco di account

L'account amministratore può utilizzare la console o l'API Detective per visualizzare un elenco di account. L'elenco può includere:

- Account che l'account amministratore ha invitato a partecipare al grafico del comportamento. Questi account hanno un tipo Su invito.
- Per il grafico di comportamento dell'organizzazione, tutti gli account dell'organizzazione. Questi account hanno un tipo Per organizzazione.

I risultati non includono gli account membri invitati che hanno rifiutato un invito o che l'account amministratore ha rimosso dal grafico del comportamento. Include solo gli account con i seguenti stati.

Verifica in corso

Per gli account invitati, Detective sta verificando l'indirizzo e-mail dell'account prima di inviare l'invito.

Per gli account dell'organizzazione, il Detective sta verificando che l'account appartenga all'organizzazione. Detective verifica inoltre che sia stato l'account amministratore di Detective ad abilitare l'account.

Verifica non riuscita

La verifica non è riuscita. L'invito non è stato inviato o l'account dell'organizzazione non è stato abilitato come membro.

Invited (Invitato)

Per gli account invitati. L'invito è stato inviato, ma l'account membro non ha ancora risposto.

Non membro

Per gli account dell'organizzazione nel grafico del comportamento dell'organizzazione. L'account dell'organizzazione non è attualmente un account membro. Non contribuisce con i dati al grafico del comportamento dell'organizzazione.

Abilitato

Per gli account invitati, l'account membro ha accettato l'invito e contribuisce i dati al grafico del comportamento.

Per gli account dell'organizzazione nel grafico del comportamento dell'organizzazione, l'account amministratore di Detective ha abilitato l'account come account membro. L'account contribuisce con i dati al grafico del comportamento dell'organizzazione.

Non abilitato

Per gli account invitati, l'account membro ha accettato l'invito, ma non può essere abilitato.

Per gli account dell'organizzazione nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective ha provato ad abilitare l'account, ma non è stato possibile.

Per gli account invitati, il Detective controlla il numero di account dei membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico del comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Detective verifica se il volume di dati rientra nella quota di Detective. Il volume di dati che fluiscono in un grafico di comportamento deve essere inferiore al massimo consentito da Detective. Se l'attuale volume importato supera il limite di 10 TB al giorno per il volume di dati del grafico del comportamento, Detective non ti consentirà di aggiungere altri account membro.

Elenco degli account (console)

Puoi usare il AWS Management Console per visualizzare e filtrare il tuo elenco di account.

Visualizzare l'elenco degli account (console)

1. Accedi alla AWS Management Console. Quindi, apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.

   L'elenco degli account membri contiene i seguenti account:

   - Il tuo account
   - Account che hai invitato a contribuire con i dati al grafico del comportamento
   - Nel grafico del comportamento dell'organizzazione, tutti gli account dell'organizzazione

   Per ogni account, l'elenco riporta le seguenti informazioni.

   - L'identificatore AWS dell'account.
   - Per gli account dell'organizzazione, il nome dell'account.
   - Il tipo di account (Per invito o Per organizzazione).
   - Per gli account invitati, l'indirizzo e-mail dell'utente root dell'account.
   - Lo stato dell'account.
   - Il volume di dati giornaliero dell'account. Detective non può recuperare il volume di dati per gli account che non sono abilitati come account membri.
   - La data dell'ultimo aggiornamento dello stato dell'account.

Puoi utilizzare le schede nella parte superiore della tabella per filtrare l'elenco in base allo stato dell'account membro. Ogni scheda mostra il numero di account membri corrispondenti.

- Scegli Tutti per visualizzare tutti gli account membri.
- Scegli Abilitato per visualizzare gli account con lo stato Abilitato.
- Scegli Non abilitato per visualizzare gli account con uno stato diverso da Abilitato.

Puoi anche aggiungere altri filtri all'elenco degli account membri.

Aggiungere un filtro all'elenco degli account nel grafico del comportamento (console)

1. Scegli la casella di filtro.
2. Scegli la colonna da utilizzare per filtrare l'elenco:
3. Per la colonna specificata, scegli il valore da utilizzare per il filtro.
4. Per rimuovere un filtro, scegli l'icona x in alto a destra.
5. Per aggiornare l'elenco con le informazioni di stato più recenti, scegli l'icona di aggiornamento in alto a destra.

Elencare gli account dei membri (Detective API, AWS CLI)

Puoi utilizzare una chiamata API o AWS Command Line Interface visualizzare un elenco di account membri nel tuo grafico comportamentale.

Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Per recuperare un elenco di account dei membri (Detective API, AWS CLI)

- API Detective: usa l'operazione `ListMembers`. Per identificare il grafico del comportamento previsto, specifica l'ARN del grafico del comportamento.

  Tieni presente che per il grafico del comportamento dell'organizzazione, `ListMembers` non restituisce gli account dell'organizzazione che non hai abilitato come account membri o che hai dissociato dal grafico del comportamento.
- AWS CLI: alla riga di comando, esegui il comando `list-members`.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Recuperare i dettagli su account membri specifici nel tuo grafico del comportamento (API Detective, AWS CLI)

- API Detective: usa l'operazione `GetMembers`. Specifica l'ARN del grafico del comportamento e l'elenco degli identificatori degli account per gli account membri.
- AWS CLI: alla riga di comando, esegui il comando `get-members`.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

Esempio:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gestione degli account dell'organizzazione come account membri

Nel grafico di comportamento dell'organizzazione, l'account amministratore di Detective determina quali account dell'organizzazione abilitare come account membri.

Può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione come account membri oppure può abilitare manualmente gli account dell'organizzazione.

L'account amministratore di Detective può anche dissociare gli account dell'organizzazione dal grafico di comportamento dell'organizzazione.

Indice

Abilitazione automatica di nuovi account dell'organizzazione come account membri

L'account amministratore di Detective può configurare Detective per abilitare automaticamente nuovi account dell'organizzazione come account membri nel grafico di comportamento dell'organizzazione.

Quando vengono aggiunti nuovi account all'organizzazione, questi vengono aggiunti all'elenco nella pagina Gestione degli account. Per gli account dell'organizzazione, Tipo è Per organizzazione.

Per impostazione predefinita, i nuovi account dell'organizzazione non sono abilitati come account membri. Il loro stato è Non membro.

Quando scegli di abilitare automaticamente gli account dell'organizzazione, Detective inizia ad abilitare nuovi account come account membri quando vengono aggiunti all'organizzazione. Detective non abilita gli account dell'organizzazione esistenti che non sono ancora abilitati.

Detective può abilitare gli account dell'organizzazione come account membro solo se il numero massimo di account membri per un grafico comportamentale è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Detective verifica se il volume di dati rientra nella quota di Detective. Il volume di dati che fluiscono in un grafico di comportamento deve essere inferiore al massimo consentito da Detective. Se l'attuale volume importato supera il limite di 10 TB al giorno, non puoi aggiungere altri account e Detective disabiliterà l'ulteriore acquisizione di dati.

Abilitazione automatica di nuovi account dell'organizzazione (console)

Sulla pagina Gestione dell'account, l'impostazione Abilita automaticamente i nuovi account dell'organizzazione determina se abilitare automaticamente i nuovi account man mano che vengono aggiunti a un'organizzazione.

Abilitare automaticamente nuovi account dell'organizzazione come account membri

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Attiva l'opzione Abilitare automaticamente i nuovi account dell'organizzazione.

Abilitazione automatica di nuovi account aziendali (Detective API, AWS CLI)

Per determinare se abilitare automaticamente nuovi account dell'organizzazione come account membri, l'account amministratore può utilizzare l'API Detective o l' AWS Command Line Interface.

Per visualizzare e gestire la configurazione, è necessario specificare l'ARN del grafico di comportamento. Per ottenere l'ARN, utilizza l'operazione `ListGraphs`.

Visualizzare la configurazione corrente per l'abilitazione automatica degli account dell'organizzazione

- API Detective: usa l'operazione `DescribeOrganizationConfiguration`.

  Nella risposta, se i nuovi account dell'organizzazione vengono abilitati automaticamente, `AutoEnable` è `true`.
- AWS CLI: alla riga di comando, esegui il comando `describe-organization-configuration`.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

  Esempio

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Abilitare automaticamente nuovi account dell'organizzazione

- API Detective: usa l'operazione `UpdateOrganizationConfiguration`. Per abilitare automaticamente nuovi account dell'organizzazione, imposta `AutoEnable` su `true`.
- AWS CLI: alla riga di comando, esegui il comando `update-organization-configuration`.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --auto-enable | --no-auto-enable
```

  Esempio

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --auto-enable
```

Abilitazione degli account dell'organizzazione come account membri

Se non abiliti automaticamente i nuovi account dell'organizzazione, puoi abilitarli manualmente. È inoltre necessario abilitare manualmente gli account che sono stati dissociati.

Determinazione se un account può essere abilitato

Non è possibile abilitare un account dell'organizzazione come account membro se il grafico di comportamento dell'organizzazione ha già un massimo di 1.200 account abilitati. In questo caso, lo stato dell'account dell'organizzazione rimane Non membro. L'account non fornisce dati al grafico di comportamento.

Non appena l'account membro può essere abilitato, Detective modifica automaticamente lo stato dell'account membro in Abilitato. Ad esempio, lo stato dell'account membro cambia in Abilitato se l'account amministratore rimuove gli account di altri membri per liberare spazio per un account.

Dissociazione degli account dell'organizzazione come account membri (console)

Dalla pagina Gestione degli account, è possibile abilitare gli account dell'organizzazione come account membri.

Abilitare gli account dell'organizzazione come account membri

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Per visualizzare l'elenco degli account che non sono attualmente abilitati, scegli Non abilitato.
4. Puoi selezionare account aziendali specifici o abilitare tutti gli account dell'organizzazione.

   Per abilitare gli account dell'organizzazione selezionati:

   a. Seleziona ogni account dell'organizzazione che desideri abilitare.
   b. Scegli Abilita account.

   Per abilitare tutti gli account dell'organizzazione, scegli Abilita tutti gli account dell'organizzazione.

Abilitazione degli account dell'organizzazione come account membro (Detective API, AWS CLI)

Puoi utilizzare l'API Detective o AWS Command Line Interface abilitare gli account dell'organizzazione come account membro nel grafico del comportamento dell'organizzazione. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Per abilitare gli account dell'organizzazione come account membro (Detective API, AWS CLI)

- API Detective: usa l'operazione `CreateMembers`. È necessario specificare l'ARN del grafico.

  Per ogni account, specifica l'identificatore dell'account. Gli account dell'organizzazione nel grafico di comportamento dell'organizzazione non ricevono un invito. Non è necessario specificare un indirizzo e-mail o altre informazioni sull'invito.
- AWS CLI: alla riga di comando, esegui il comando `create-members`.

  ```
  aws detective create-members --accounts AccountId=<AWS account ID> --graph-
  arn <behavior graph ARN>
  ```

  Esempio

  ```
  aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012
   --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
  ```

Dissociazione degli account dell'organizzazione come account membri

Per interrompere l'importazione di dati da un account dell'organizzazione nel grafico di comportamento dell'organizzazione, puoi dissociare l'account. I dati esistenti per quell'account rimangono nel grafico di comportamento.

Quando si dissocia un account dell'organizzazione, lo stato cambia in Non membro. Detective interrompe l'importazione di dati da quell'account, ma l'account rimane nell'elenco.

Dissociazione degli account dell'organizzazione (console)

Dalla pagina Gestione degli account, è possibile dissociare gli account dell'organizzazione come account membri.

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Per visualizzare l'elenco degli account abilitati, scegli Abilitato.
4. Seleziona la casella di controllo per ogni account da dissociare.
5. Scegli Azioni. Quindi scegli Disabilita account.

   Lo stato dell'account per gli account dissociati cambia in Non membro.

Dissociazione degli account aziendali (Detective API,) AWS CLI

Puoi utilizzare l'API Detective o AWS Command Line Interface per dissociare gli account dell'organizzazione dagli account dei membri nel tuo grafico comportamentale.

Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Dissociare gli account dell'organizzazione dal grafico di comportamento dell'organizzazione (API Detective, AWS CLI)

- API Detective: usa l'operazione `DeleteMembers`. Specifica l'ARN del grafico e l'elenco degli identificatori degli account per gli account membri da dissociare.
- AWS CLI: alla riga di comando, esegui il comando `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Esempio

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gestione degli account membri invitati

Un account amministratore può invitare gli account a diventare account membri in un grafico di comportamento Quando un account membro accetta l'invito ed è abilitato, Amazon Detective inizia a importare ed estrarre i dati dell'account membro in quel grafico di comportamento.

Per i grafici di comportamento diversi dal grafico di comportamento dell'organizzazione, tutti gli account membri sono account invitati.

L'account amministratore di Detective può anche invitare account che non sono account dell'organizzazione al grafico di comportamento dell'organizzazione.

L'account amministratore può rimuovere gli account membri invitati dal grafico di comportamento.

Indice

Invito degli account membri a un grafico di comportamento

L'account amministratore può invitare gli account a contribuire con i propri dati al grafico di comportamento. Un grafico di comportamento può contenere fino a 1.200 account membri.

A un livello superiore, la procedura per invitare gli account a contribuire a un grafico di comportamento è la seguente.

1. Per ogni account membro da aggiungere, l'account amministratore fornisce l'identificatore AWS dell'account e l'indirizzo e-mail dell'utente root.
2. Detective verifica che l'indirizzo e-mail sia l'indirizzo e-mail dell'utente root per l'account. Se le informazioni sull'account sono valide, Detective invia l'invito all'account membro.

   Detective non esegue questa convalida né invia inviti via e-mail agli account dei membri nelle seguenti regioni:

   - AWS GovCloud Regione (Stati Uniti orientali)
   - AWS GovCloud Regione (Stati Uniti occidentali)

   Per le altre regioni, puoi `DisableEmailNotification` utilizzare il CreateMembersfunzionamento dell'API Detective. Se `DisableEmailNotification` è impostato su true, Detective non invierà inviti agli account dei membri. Si tratta di un'impostazione utile per gli account gestiti centralmente.
3. L'account membro accetta o rifiuta l'invito.

Anche se l'account amministratore non invia e-mail di invito, l'account membro deve comunque rispondere all'invito.

4. Dopo che l'account membro ha accettato l'invito, Detective inizia a inserire i dati dell'account del membro nel grafico del comportamento.
5. Non appena l'account membro può essere abilitato, Detective ne modifica automaticamente lo stato in Abilitato.

   Ad esempio, lo stato dell'account membro cambia in Abilitato se l'account amministratore rimuove gli account di altri membri per liberare spazio per un account.

   Se più di un account non è abilitato, Detective abilita gli account nell'ordine in cui sono stati invitati. Il processo per verificare se abilitare gli account non abilitati viene eseguito ogni ora.

   L'account amministratore può anche abilitare gli account manualmente anziché attendere il processo automatico. Ad esempio, l'account amministratore potrebbe voler selezionare gli account da abilitare. Per informazioni, consulta the section called “Abilitazione di un account membro che non è abilitato”.

   Tieni presente che Detective ha iniziato ad abilitare automaticamente gli account che non sono abilitati il 12 maggio 2021. Gli account che non erano abilitati prima di allora non vengono abilitati automaticamente. L'account amministratore li deve abilitare manualmente.

Invito di singoli account a un grafico di comportamento (console)

Puoi specificare manualmente gli account membri da invitare per contribuire con i loro dati a un grafico di comportamento.

Selezionare manualmente gli account membri da invitare (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Scegli Azioni. Quindi scegli Invita account.
4. In Aggiungi account, scegli Aggiungi singoli account.
5. Per aggiungere un account membro all'elenco degli inviti, procedi nel seguente modo.

   a. Scegli Aggiungi account.

   b. Per ID AWS account, inserisci l'ID AWS dell'account.

c. Per Indirizzo e-mail, immetti l'indirizzo e-mail dell'utente root per l'account.

6. Per rimuovere un account dall'elenco, scegli Rimuovi per quell'account.
7. In Personalizza e-mail di invito, aggiungi contenuti personalizzati da includere nell'e-mail di invito.

   Ad esempio, puoi utilizzare quest'area per fornire le informazioni di contatto. Oppure per ricordare all'account membro che deve collegare la policy IAM richiesta al proprio utente o ruolo prima di poter accettare l'invito.
8. Il campo Policy IAM dell'account membro contiene il testo della policy IAM richiesta per gli account membri. L'e-mail di invito include questo testo della policy. Per copiare il testo della policy, scegli Copia.
9. Seleziona Invite (Invita).

Invito di un elenco di account membri a un grafico di comportamento (console)

Dalla console Detective, puoi fornire un file `.csv` contenente un elenco di account membri da invitare al tuo grafico di comportamento.

La prima riga nel file è la riga di intestazione. Ogni account viene quindi riportato su una riga separata. Ogni voce relativa all'account membro contiene l'ID AWS dell'account e l'indirizzo e-mail dell'utente root dell'account.

Esempio:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Quando Detective elabora il file, ignora gli account già invitati, a meno che lo stato dell'account non sia Verifica non riuscita. Questo stato indica che l'indirizzo e-mail fornito per l'account non corrispondeva all'indirizzo e-mail dell'utente root dell'account. In tal caso, Detective elimina l'invito originale e riprova per verificare l'indirizzo e-mail e inviare l'invito.

Questa opzione fornisce anche un modello da utilizzare per creare l'elenco di account.

Invitare gli account membri da un elenco .csv (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.

2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Scegli Azioni. Quindi scegli Invita account.
4. In Aggiungi account, scegli Aggiungi da .csv.
5. Per scaricare un file modello da cui lavorare, scegli Scarica modello in formato .csv.
6. Per selezionare il file contenente l'elenco degli account, scegli Scegli il file .csv.
7. In Rivedi gli account membri, verifica l'elenco degli account membri che Detective ha trovato nel file.
8. In Personalizza e-mail di invito, aggiungi contenuti personalizzati da includere nell'e-mail di invito.

   Ad esempio, puoi fornire le informazioni di contatto o ricordare all'account membro la policy IAM richiesta.
9. Il campo Policy IAM dell'account membro contiene il testo della policy IAM richiesta per gli account membri. L'e-mail di invito include questo testo della policy. Per copiare il testo della policy, scegli Copia.
10. Seleziona Invite (Invita).

Invitare gli account dei membri a un grafico comportamentale (Detective API, AWS CLI)

Puoi utilizzare l'API Detective o AWS Command Line Interface invitare gli account dei membri a contribuire con i loro dati a un grafico del comportamento. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Per invitare gli account dei membri a un grafico comportamentale (Detective API, AWS CLI)

- API Detective: usa l'operazione `CreateMembers`. È necessario specificare l'ARN del grafico. Per ogni account, specifica l'identificatore dell'account e l'indirizzo e-mail dell'utente root.

  Per non inviare le e-mail di invito agli account membri, imposta `DisableEmailNotification` su true. Per impostazione predefinita, `DisableEmailNotification` è false.

  Se invii le e-mail di invito, puoi facoltativamente fornire un testo personalizzato da aggiungere all'e-mail di invito.
- AWS CLI: alla riga di comando, esegui il comando `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message
 text>"
```

Esempio

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

Per indicare di non inviare le e-mail di invito agli account membri, includi `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

Esempio

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Aggiungere un elenco di account membri tra le regioni (script Python attivo) GitHub

Detective fornisce uno script open source GitHub che consente di effettuare le seguenti operazioni:

- Aggiungi un elenco specifico di account membri ai grafici di comportamento di un account amministratore in un elenco specifico di Regioni.
- Se l'account amministratore non dispone di un grafico di comportamento in una Regione, lo script abilita anche Detective e crea il grafico di comportamento in quella Regione.
- Invia le e-mail di invito agli account membri.
- Accetta automaticamente gli inviti per gli account membri.

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. Utilizzo degli script Python di Amazon Detective

Abilitazione di un account membro che non è abilitato

Dopo che un account membro ha accettato un invito, Amazon Detective verifica il numero di account membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account. Se Detective non è in grado di abilitare l'account membro, imposta lo stato dell'account membro su Non abilitato.

Gli account membri che non sono abilitati non contribuiscono con i dati al grafico di comportamento.

Detective abilita automaticamente gli account in quanto il grafico di comportamento è in grado di gestirli.

Puoi anche provare ad abilitare manualmente gli account membri che sono account membri non abilitati. Ad esempio, potresti rimuovere gli account membri esistenti per ridurre il volume di dati. Invece di attendere il processo automatico che abilita gli account, puoi provare ad abilitare gli account membro con stato Non abilitato.

Abilitazione di un account membro non abilitato (console)

L'elenco degli account membri include un'opzione per abilitare gli account membri selezionati il cui stato è Non abilitato.

Abilitare un account membro che non è abilitato

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account membro, seleziona la casella di controllo per ogni account membro da abilitare.

   Puoi abilitare solo gli account membri con lo stato Non abilitato.
4. Scegli Abilita account.

Detective determina se l'account membro può essere abilitato. Se l'account membro può essere abilitato, lo stato cambia in Abilitato.

Attivazione di un account membro non abilitato (Detective API, AWS CLI)

È possibile utilizzare una chiamata API o abilitare un account AWS Command Line Interface a membro singolo che non è abilitato. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Abilitare un account membro che non è abilitato

- API Detective: usa l'operazione API `StartMonitoringMember`. È necessario fornire l'ARN del grafico di comportamento. Per identificare l'account membro, utilizza l'identificatore AWS dell'account.
- AWS CLI: alla riga di comando, esegui il comando `start-monitoring-member`:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

Per esempio:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Rimozione degli account membri invitati da un grafico di comportamento

L'account amministratore può rimuovere gli account membri da un grafico di comportamento in qualsiasi momento.

Detective rimuove automaticamente gli account dei membri che vengono chiusi AWS, ad eccezione delle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).

Quando un account membro invitato viene rimosso da un grafico di comportamento, si verifica quanto segue.

- L'account membro viene rimosso da I miei account membro.
- Amazon Detective interrompe l'importazione dei dati dall'account rimosso.

Detective non rimuove alcun dato esistente dal grafico di comportamento, che aggrega i dati tra gli account membri.

Rimozione degli account membri invitati da un grafico di comportamento (console)

Puoi utilizzare il AWS Management Console per rimuovere gli account dei membri invitati dal tuo grafico comportamentale.

Rimuovere gli account membri (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. Nell'elenco di account, seleziona la casella di controllo accanto a ciascun account membro da rimuovere.

   Non puoi rimuovere il tuo account dall'elenco.
4. Scegli Azioni. Quindi scegli Disabilita account.

Rimozione degli account dei membri invitati da un grafico comportamentale (Detective API, AWS CLI)

Puoi utilizzare l'API Detective o AWS Command Line Interface rimuovere gli account dei membri invitati dal tuo grafico comportamentale. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Per rimuovere gli account dei membri invitati dal tuo grafico comportamentale (Detective API, AWS CLI)

- API Detective: usa l'operazione `DeleteMembers`. Specifica l'ARN del grafico e l'elenco degli identificatori degli account per gli account membri da rimuovere.
- AWS CLI: alla riga di comando, esegui il comando `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Esempio:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Rimozione di un elenco di account membri invitati in tutte le regioni (script Python attivo) GitHub

Detective fornisce uno script open source in GitHub. È possibile utilizzare questo script per rimuovere un elenco specifico di account membri dai grafici di comportamento di un account amministratore in un elenco specifico di Regioni.

Per informazioni su come configurare e utilizzare GitHub gli script, vedere. Utilizzo degli script Python di Amazon Detective

Per gli account membri: gestione degli inviti e delle iscrizioni al grafico di comportamento

Amazon Detective addebita a ciascun account membro i dati importati per ogni grafico di comportamento a cui contribuisce.

La pagina Gestione dell'account consente agli account membri di visualizzare gli account amministratore per i grafici di comportamento di cui sono membri.

Gli account membri invitati a un grafico di comportamento possono visualizzare e rispondere ai relativi inviti. Possono anche rimuovere il proprio account dal grafico.

Per quanto riguarda il grafico di comportamento dell'organizzazione, gli account dell'organizzazione non controllano se il loro account è un account membro. L'account amministratore di Detective sceglie gli account dell'organizzazione da abilitare o disabilitare come account membri.

Indice

Policy IAM richiesta per un account membro

Prima che un account membro possa visualizzare e gestire gli inviti, è necessario collegare la policy IAM richiesta al relativo principale. Il principale può essere un utente o un ruolo esistente oppure puoi crearne uno nuovo da utilizzare per Detective.

Idealmente, l'account amministratore deve far sì che l'amministratore IAM colleghi la policy richiesta.

La policy IAM dell'account membro concede l'accesso alle operazioni dell'account membro in Amazon Detective. L'e-mail di invito a contribuire a un grafico di comportamento include il testo di tale policy IAM.

Per utilizzare questa policy, sostituire *<behavior graph ARN>* con l'ARN del grafico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Tieni presente che gli account dell'organizzazione nel grafico di comportamento dell'organizzazione non ricevono inviti e non possono dissociare il loro account dal grafico. Se non appartengono ad altri grafici di comportamento, richiedono solo l'autorizzazione `ListInvitations`. `ListInvitations` consente loro di visualizzare l'account amministratore per il grafico di comportamento. Le autorizzazioni per gestire gli inviti e annullare le iscrizioni si applicano solo alle iscrizioni su invito.

Visualizzazione dell'elenco degli inviti del grafico di comportamento

Dalla console Amazon Detective, dall'API Detective o AWS Command Line Interface dall'account di un membro può vedere gli inviti relativi al grafico del comportamento.

Visualizzazione degli inviti del grafico di comportamento (console)

Puoi visualizzare gli inviti con un grafico comportamentale da. AWS Management Console

Visualizzare gli inviti del grafico di comportamento (console)

1. Accedi alla AWS Management Console. Quindi, apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.

Nella pagina Gestione dell'account, I miei account amministratore contiene gli inviti del grafico di comportamento aperti e accettati nella Regione corrente. Per un account dell'organizzazione, I miei account amministratore contiene anche il grafico di comportamento dell'organizzazione.

Se il tuo account è attualmente nel periodo di prova gratuita, la pagina mostra anche il numero di giorni rimanenti della prova.

L'elenco non contiene gli inviti che hai rifiutato, gli abbonamenti per cui ti sei cancellato o gli abbonamenti rimossi dall'amministratore.

Ogni invito mostra il numero di account amministratore, la data di accettazione dell'invito e lo stato corrente dell'invito.

- Per gli inviti a cui non hai risposto, lo stato è Invitato.
- Per gli inviti che hai accettato, lo stato è Abilitato o Non abilitato.

  Se lo stato è Abilitato, il tuo account contribuisce con i dati al grafico di comportamento.

  Se lo stato è Non abilitato, l'account non fornisce dati al grafico di comportamento.

  Se il tuo account non fa sì che il grafico del comportamento superi la quota di Detective, Detective aggiorna lo stato del tuo account su Attivato. Altrimenti, lo stato rimane Non abilitato.

  Se il grafico di comportamento è in grado di adattarsi al volume di dati del tuo account, Detective lo aggiorna automaticamente su Abilitato. Ad esempio, l'account amministratore potrebbe

rimuovere gli account di altri membri in modo che il tuo account possa essere abilitato. L'account amministratore può anche abilitare l'account manualmente.

Visualizzazione degli inviti del grafico di comportamento (API Detective, AWS CLI)

Puoi elencare gli inviti del grafico di comportamento dall'API Detective o dalla AWS Command Line Interface.

Recuperare un elenco di inviti aperti e accettati ai grafici di comportamento (API Detective, AWS CLI)

- API Detective: usa l'operazione `ListInvitations`.
- AWS CLI: alla riga di comando, esegui il comando `list-invitations`.

```
aws detective list-invitations
```

Risposta a un invito del grafico di comportamento

Dopo aver accettato un invito, il Detective controlla il numero di account dei membri. Il numero massimo di account membri per un grafico di comportamento è 1.200. Se il grafico di comportamento contiene già 1.200 account membri, non è possibile abilitare nuovi account.

Dopo aver accettato l'invito, Detective sarà abilitato nel tuo account. Detective verifica se il volume di dati rientra nella quota di Detective. Il volume di dati che fluiscono in un grafico di comportamento deve essere inferiore al massimo consentito da Detective. Se l'attuale volume importato supera il limite di 10 TB al giorno, non puoi aggiungere altri account e Detective disabiliterà l'ulteriore acquisizione di dati. La console Detective visualizza una notifica per indicare che il volume di dati è troppo grande e lo stato rimane Non abilitato.

Se rifiuti l'invito, questo viene rimosso dal tuo elenco di inviti e Detective non utilizzerà i dati del tuo account nel grafico di comportamento.

Risposta a un invito del grafico di comportamento (console)

Puoi usare il AWS Management Console per rispondere all'e-mail di invito, che include un link alla console Detective. Puoi rispondere solo a un invito con lo stato Invitato.

Rispondere a un invito del grafico di comportamento (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.

2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account di amministratore, per accettare l'invito e iniziare a contribuire con i dati al grafico di comportamento, scegli Accetta invito.

   Per rifiutare l'invito e rimuoverlo dall'elenco, scegli Rifiuta.

Risposta a un invito con grafico comportamentale (Detective API, AWS CLI)

Puoi rispondere agli inviti del grafico di comportamento dall'API Detective o dalla AWS Command Line Interface.

Per accettare un invito al grafico comportamentale (Detective API, AWS CLI)

- API Detective: usa l'operazione `AcceptInvitation`. È necessario specificare l'ARN del grafico.
- AWS CLI: alla riga di comando, esegui il comando `accept-invitation`.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Per rifiutare un invito a un grafico comportamentale (Detective API, AWS CLI)

- API Detective: usa l'operazione `RejectInvitation`. È necessario specificare l'ARN del grafico.
- AWS CLI: alla riga di comando, esegui il comando `reject-invitation`.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Rimozione dell'account da un grafico di comportamento

Dopo aver accettato un invito, puoi rimuovere il tuo account da un grafico di comportamento in qualsiasi momento. Quando rimuovi il tuo account da un grafico di comportamento, Amazon Detective interrompe l'importazione dei dati dal tuo account nel grafico di comportamento. I dati esistenti rimangono nel grafico di comportamento.

Solo gli account invitati possono rimuovere il proprio account da un grafico di comportamento. Gli account dell'organizzazione non possono rimuovere il proprio account dal grafico di comportamento dell'organizzazione.

Rimozione dell'account da un grafico di comportamento (console)

Puoi usare il AWS Management Console per rimuovere il tuo account da un grafico comportamentale.

Rimuovere l'account da un grafico di comportamento (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, scegli Gestione account.
3. In I miei account di amministratore, per il grafico di comportamento a cui desideri rinunciare, scegli Abbandona.

Rimuovere l'account da un grafico comportamentale (Detective API, AWS CLI)

Puoi utilizzare l'API Detective o AWS Command Line Interface rimuovere il tuo account da un grafico comportamentale.

Per rimuovere il tuo account da un grafico comportamentale (Detective API, AWS CLI)

- API Detective: usa l'operazione `DisassociateMembership`. È necessario specificare l'ARN del grafico.
- AWS CLI: alla riga di comando, esegui il comando `disassociate-membership`.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Esempio:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Effetto delle operazioni dell'account sui grafici di comportamento

Queste operazioni hanno i seguenti effetti sui dati e sull'accesso ad Amazon Detective.

Detective disabilitato

Quando un account amministratore disabilita Detective, si verifica quanto segue:

- Il grafico di comportamento viene rimosso.
- Detective interrompe l'importazione dei dati dall'account amministratore e dagli account membri per quel grafico di comportamento.

Account membro rimosso dal grafico di comportamento

Quando un account membro viene rimosso da un grafico di comportamento, Detective interrompe l'importazione dei dati da quell'account.

I dati esistenti nel grafico di comportamento non vengono modificati.

Per gli account invitati, l'account viene rimosso dall'elenco I miei account membri.

Per gli account dell'organizzazione nel grafico di comportamento dell'organizzazione, lo stato dell'account cambia in Non membro.

L'account del membro lascia l'organizzazione

Quando un account membro lascia un'organizzazione, si verifica quanto segue:

- L'account viene rimosso dall'elenco I miei account membro per il grafico di comportamento dell'organizzazione.
- Detective interrompe l'importazione dei dati dall'account.

I dati esistenti nel grafico di comportamento non vengono modificati.

Account AWS sospeso

Quando un account amministratore viene sospeso in AWS, perde l'autorizzazione a visualizzare il grafico di comportamento in Detective. Detective smette di importare i dati nel grafico di comportamento.

Quando un account membro viene sospeso in AWS, Detective interrompe l'importazione dei dati per quell'account.

Dopo 90 giorni, l'account viene chiuso o riattivato. Quando un account amministratore viene riattivato, le relative autorizzazioni di Detective vengono ripristinate. Detective riprende l'importazione dei dati dall'account. Quando un account membro viene riattivato, Detective riprende l'importazione dei dati dall'account.

Account AWS chiuso

Quando un account AWS viene chiuso, Detective risponde alla chiusura come riportato di seguito.

- Per un account amministratore, Detective elimina il grafico di comportamento.
- Per un account membro, Detective rimuove l'account dal grafico di comportamento.

AWS manterrà i dati della policy dell'account per 90 giorni a partire dalla data di validità della chiusura dell'account amministratore. Al termine del periodo di 90 giorni, AWS elimina definitivamente tutti i dati delle policy per l'account.

- Per conservare i risultati per più di 90 giorni, puoi archiviare le policy. È inoltre possibile utilizzare un'operazione personalizzata con una regola EventBridge per memorizzare i risultati in un bucket S3.
- Finché AWS conserva i dati delle policy, quando si riapre l'account chiuso, AWS riassegna l'account come amministratore del servizio e recupera i dati delle policy di servizio per l'account.
- Per ulteriori informazioni, consulta Chiusura di un account.

> **Important**
>
> Per i clienti nelle regioni AWS GovCloud (US):

- Prima di chiudere il tuo account, effettua il backup ed elimina le risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

Monitoraggio delle azioni e dell'utilizzo in Amazon Detective

Per aiutarti a tenere traccia delle tue attività di Detective, la pagina Utilizzo mostra la quantità di dati importati e il costo previsto.

- Per gli account amministratore, la pagina Utilizzo mostra il volume dei dati e il costo previsto nell'intero grafico di comportamento.
- Per gli account membri, la pagina Utilizzo mostra il volume di dati e il costo previsto per l'account in base ai grafici del comportamento a cui contribuiscono.

Detective supporta anche la registrazione AWS CloudTrail.

Indice

Monitoraggio dell'utilizzo e dei costi per un grafico di comportamento (account amministratore)

Amazon Detective fattura a ciascun account i dati utilizzati in ogni grafico di comportamento a cui appartiene l'account. Detective applica una tariffa fissa a più livelli per GB per tutti i dati indipendentemente dall'origine.

Per gli account amministratore, la pagina Utilizzo della console di Detective consente di visualizzare il volume di dati importati per origine dati o per account nei 30 giorni precedenti. Gli account amministratore visualizzano anche un costo previsto per un periodo tipico di 30 giorni per il rispettivo account e per l'intero grafico di comportamento.

Visualizzazione delle informazioni sull'utilizzo di Detective

1. Accedere alla AWS Management Console. Quindi, apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Utilizzo.

3. Scegli una scheda per selezionare tra la visualizzazione dell'utilizzo per origine dati o per account.

Volume di dati importati per ogni account

Volume acquisito per account membro riporta gli account attivi nel grafico di comportamento. Non riporta gli account dei membri che sono stati rimossi.

Per ogni account, l'elenco dei volumi importati fornisce le seguenti informazioni.

- L'identificatore dell'account AWS e l'indirizzo e-mail dell'utente root.
- La data in cui l'account ha iniziato a fornire dati al grafico di comportamento.

  Per l'account amministratore, questa è la data in cui l'account ha abilitato Detective.

  Per gli account membro, questa è la data in cui un account è stato abilitato come account membro dopo aver accettato l'invito.
- Il volume di dati importati dall'account nei 30 giorni precedenti. Il totale include tutti i tipi di origine.
- Se l'account si trova nel periodo di prova gratuito. Per gli account che si trovano nel periodo di prova gratuito, l'elenco mostra il numero di giorni rimanenti.

  Se nessuno degli account è nel periodo di prova gratuito, la colonna relativa allo stato della prova gratuita non viene visualizzata.

Costi previsti per il grafico di comportamento

Costo previsto di questo account mostra il costo previsto per 30 giorni di dati per l'account amministratore. Il costo previsto si basa sul volume medio giornaliero per ogni account amministratore.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati dell'account amministratore per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Per informazioni, consultare the section called “Come Detective calcola il costo previsto”.

Costo previsto per il grafico di comportamento

Costo previsto di tutti gli account mostra un costo mostra un costo totale previsto per 30 giorni di dati per l'intero grafico di comportamento. Il costo previsto si basa sul volume medio giornaliero per ogni account.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati del grafico di comportamento per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Il costo previsto non include gli account membri che sono stati rimossi dal grafico di comportamento. Per informazioni, consultare the section called “Come Detective calcola il costo previsto”.

Volume di dati importati dai pacchetti di origine

Seleziona Per pacchetto sorgente per visualizzare il volume di dati importati elencato dai diversi pacchetti sorgente abilitati nel grafico di comportamento.

Tutti gli account possono visualizzare questi dati per i propri account. Un account amministratore può visualizzare pannelli aggiuntivi che elencano l'utilizzo per pacchetto sorgente per ciascun membro. Non riporta gli account dei membri che sono stati rimossi.

Core Detective

I pannelli core di Detective mostrano il volume di dati importati dalle origini principali di Detective (log di CloudTrail, log di flusso VPC e risultati di GuardDuty) negli ultimi 30 giorni.

Log di controllo EKS

I pannelli dei log di controllo EKS mostrano il volume di dati importati dalle origini dei log di controllo EKS negli ultimi 30 giorni. I pannelli per questo pacchetto di origine sono disponibili solo se i log di controllo EKS sono abilitati per il grafico di comportamento.

Monitoraggio dell'utilizzo e dei costi attraverso i grafici del comportamento (account membro)

Amazon Detective fattura a ciascun account i dati utilizzati in ogni grafico di comportamento a cui appartiene l'account. Detective applica una tariffa fissa a più livelli per GB per tutti i dati indipendentemente dall'origine.

Per gli account membri, la pagina Utilizzo mostra il volume di dati e il costo previsto per 30 giorni solo per quell'account.

Visualizzazione delle informazioni sull'utilizzo di Detective

1. Accedere alla AWS Management Console. Quindi, apri la console Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Utilizzo.

Volume importato per ogni grafico di comportamento

Volume acquisito di questo account riporta i grafici del comportamento a cui contribuisce l'account membro. Non include gli abbonamenti per cui ti sei cancellato o gli abbonamenti rimossi dall'account amministratore.

Per ciascun grafico del comportamento, l'elenco include le seguenti informazioni.

- Il numero di account dell'account amministratore
- Il volume di dati importati dall'account membro nei 30 giorni precedenti. Il totale include tutti i tipi di origine.
- La data in cui l'account membro è stato abilitato per il grafico di comportamento.

Costo previsto nei grafici del comportamento

Costo previsto di questo account mostra il costo previsto per 30 giorni di dati per l'account membro in tutti i grafici del comportamento a cui contribuisce. Il costo previsto si basa sul volume medio giornaliero per ogni account membro.

> **Important**
>
> Questo importo è solo un costo previsto. Proietta il costo totale dei dati dell'account amministratore per un periodo di tempo tipico di 30 giorni. Si basa sull'utilizzo dei 30 giorni precedenti. Per informazioni, consultare the section called “Come Detective calcola il costo previsto”.

Come Amazon Detective calcola il costo previsto

Per calcolare i valori di costo previsti visualizzati nella pagina Utilizzo, Detective effettua le seguenti operazioni.

1. Per ottenere il costo previsto per un singolo account in un grafico del comportamento, Detective effettua le seguenti operazioni.
   a. Calcola il volume medio giornaliero. Aggiunge il volume di dati di tutti i giorni attivi e quindi lo divide per il numero di giorni in cui l'account è stato attivo.

      Se l'account è stato abilitato più di 30 giorni fa, il numero di giorni è 30. Se l'account è stato abilitato meno di 30 giorni fa, allora è il numero di giorni trascorsi dalla data di accettazione.

      Ad esempio, se l'account è stato abilitato 12 giorni fa, Detective aggiunge il volume importato per quei 12 giorni e poi lo divide per 12.
   b. Moltiplica la media giornaliera dell'account per 30. Si tratta dell'utilizzo previsto per 30 giorni dell'account.
   c. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo previsto per 30 giorni.
2. Per ottenere il costo totale previsto per un grafico di comportamento, Detective effettua le seguenti operazioni:
   a. Combina l'utilizzo previsto per 30 giorni di tutti gli account nel grafico di comportamento.
   b. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo totale previsto per 30 giorni.
3. Per ottenere il costo totale previsto per un account membro tra grafici del comportamento, Detective effettua le seguenti operazioni:
   a. Combina l'utilizzo previsto per 30 giorni di tutti gli account nel grafico del comportamento.

b. Utilizza il modello di prezzo corrispondente per calcolare il costo previsto per 30 giorni per l'utilizzo totale previsto per 30 giorni.

4. Se utilizzi un Amazon VPC condiviso, Detective calcola il costo previsto in base all'attività di monitoraggio. Consigliamo di esaminare i costi previsti per le indagini specifiche dell'ambiente.

   a. Se un account membro di Detective dispone di un Amazon VPC condiviso e ci sono altri account non Detective che utilizzano il VPC condiviso, Detective monitorerà tutto il traffico proveniente da quel VPC. L'utilizzo e il costo aumenteranno e Detective fornirà la visualizzazione di tutto il flusso di traffico all'interno del VPC.

   b. Se hai un'istanza EC2 all'interno di un Amazon VPC condiviso e il proprietario condiviso non è un membro di Detective, Detective non monitorerà alcun traffico proveniente dal VPC e l'utilizzo e i costi diminuiranno. Se desideri visualizzare il flusso di traffico all'interno del VPC, devi aggiungere il proprietario dell'Amazon VPC come membro del grafico di Detective.

Registrazione delle chiamate API di Amazon Detective con AWS CloudTrail

Detective è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Detective. CloudTrail acquisisce tutte le chiamate API per Detective come eventi. Le chiamate acquisite includono le chiamate dalla console di Detective e le chiamate di codice alle operazioni delle API Detective.

- Se viene creato un percorso, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Detective.
- Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella console di CloudTrail in Cronologia eventi.

Con le informazioni raccolte da CloudTrail, è possibile determinare:

- La richiesta effettuata a Detective
- L'indirizzo IP dal quale è stata effettuata la richiesta
- L'utente che ha effettuato la richiesta
- Quando è stata effettuata
- Dettagli aggiuntivi relativi alla richiesta

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni su Detective in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Detective, tale attività viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per Detective, crea un percorso. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3.

Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Puoi anche configurare altri servizi AWS per analizzare ulteriormente e usare i dati raccolti nei log CloudTrail.

Per ulteriori informazioni, consulta gli argomenti seguenti:

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

CloudTrail registra tutte le operazioni di Detective, descritte nella Documentazione di riferimento delle API di Detective.

Ad esempio, le chiamate alle operazioni `CreateMembers`, `AcceptInvitation` e `DeleteMembers` generano voci nei file di log di CloudTrail.

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 le credenziali utente AWS Identity and Access Management (IAM) o 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, consulta l'argomento relativo all'elemento userIdentity di CloudTrail.

Informazioni sulle voci dei file di log di Detective

Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log.

Un evento rappresenta una singola richiesta da un'origine. Gli eventi includono le informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log CloudTrail non sono una traccia stack ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `AcceptInvitation`.


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
```

```
        },
```

Gestione dei tag per un grafico di comportamento

Puoi assegnare tag al tuo grafico di comportamento. Puoi quindi utilizzare i valori dei tag nelle policy IAM per gestire l'accesso alle funzioni del grafico di comportamento in Detective. Per informazioni, consultare the section called “Autorizzazione basata sui tag del grafici di comportamento di Detective”.

Puoi anche utilizzare i tag come strumento per la rendicontazione dei costi. Ad esempio, per tenere traccia dei costi associati alla sicurezza, puoi assegnare lo stesso tag al grafico di comportamento di Detective, alla risorsa dell'hub AWS Security Hub e ai rilevatori Amazon GuardDuty. In AWS Cost Explorer, puoi quindi cercare quel tag per visualizzare una visione consolidata dei costi di tali risorse.

Visualizzazione dei tag per un grafico di comportamento (console)

Puoi gestire i tag per il tuo grafico di comportamento dalla pagina Generale.

Visualizzare l'elenco dei tag assegnati al grafico di comportamento

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).

Elencare i tag per un grafico di comportamento (API Detective, AWS CLI)

Puoi usare l'API Detective o la AWS Command Line Interface per ottenere l'elenco dei tag per il tuo grafico di comportamento.

Ottenere l'elenco di tag per un grafico di comportamento (API Detective, AWS CLI)

- API Detective: usa l'operazione `ListTagsForResource`. È necessario fornire l'ARN del grafico di comportamento.
- AWS CLI: alla riga di comando, esegui il comando `list-tags-for-resource`.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Esempio

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Aggiunta di tag a un grafico di comportamento (console)

Dall'elenco dei tag nella pagina Generale, è possibile aggiungere valori di tag al grafico di comportamento.

Aggiungere un tag al grafico di comportamento

1. Scegliere Aggiungi nuovo tag.
2. Per Chiave, inserisci il nome del tag.
3. In Valore, immetti il valore del tag.

Aggiunta di tag a un grafico di comportamento (API Detective, AWS CLI)

Puoi utilizzare l'API Detective o l'AWS CLI per aggiungere valori di tag al tuo grafico di comportamento.

Aggiungere tag a un grafico di comportamento (API Detective, AWS CLI)

- API Detective: usa l'operazione `TagResource`. Fornisci l'ARN del grafico di comportamento e i valori dei tag da aggiungere.
- AWS CLI: alla riga di comando, esegui il comando `tag-resource`.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Esempio

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Rimozione dei tag da un grafico di comportamento (console)

Per rimuovere un tag dall'elenco nella pagina Generale, scegli l'opzione Rimuovi per quel tag.

Rimozione di tag da un grafico di comportamento (API Detective, AWS CLI)

Puoi utilizzare l'API Detective o l'AWS CLI per rimuovere i valori di tag dal tuo grafico di comportamento.

Rimuovere i tag da un grafico di comportamento (API Detective, AWS CLI)

- API Detective: usa l'operazione `UntagResource`. Fornisci l'ARN del grafico di comportamento e i nomi dei tag da rimuovere.
- AWS CLI: alla riga di comando, esegui il comando `untag-resource`.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Esempio

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Sicurezza in Amazon Detective

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza.

  I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformità AWS.

  Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Detective, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione descrive come applicare il modello di responsabilità condivisa quando si utilizza Detective. I seguenti argomenti illustrano come configurare Detective per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi AWS per monitorare e proteggere le risorse Detective.

Indice

- Best practice di sicurezza per Amazon Detective

Protezione dei dati in Amazon Detective

Il modello di responsabilità condivisa di AWS si applica alla protezione dei dati in Amazon Detective. Come descritto in questo modello, AWSè responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. 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.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o 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.
- Utilizza 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 le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in 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 necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso 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. Questo include quando si lavora con Detective o con altri Servizi AWS utilizzando la console, l'API, la AWS CLI o gli SDK AWS. 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.

Detective crittografa tutti i dati che elabora e archivia a riposo e in transito.

Indice

Gestione delle chiavi per Amazon Detective

Poiché Detective non memorizza dati personali dei clienti, utilizza Chiavi gestite da AWS.

Questo tipo di chiave KMS può essere utilizzato su più account. Consulta la descrizione delle chiavi AWS di proprietà nella Guida per gli sviluppatori di AWS Key Management Service.

Questo tipo di chiave KMS ruota automaticamente ogni anno (circa 365 giorni). Consulta la descrizione della rotazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service.

Identity and Access Management per Amazon Detective

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse Detective. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Indice

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in Detective.

Utente del servizio: se utilizzi il servizio Detective per eseguire il tuo processo, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità di Detective 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 di Detective, consulta Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Detective.

Amministratore del servizio: se sei il responsabile delle risorse Detective presso la tua azienda, probabilmente disponi dell'accesso completo a Detective. Il tuo compito è determinare le funzionalità e le risorse di Detective 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 Detective, consulta Funzionamento di Amazon Detective con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a Detective. Per visualizzare policy basate su identità di Detective di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate sull'identità per Amazon Detective.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWStramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Consoleo al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue

credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'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.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi 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.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente 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 Amministratori IAM 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 all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure 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, per alcuni dei Servizi AWS, è possibile collegare 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 multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene 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 effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. 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 assunto da un servizio per eseguire operazioni per conto dell'utente. 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 ai servizi sono visualizzati nell'account Account AWSe 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: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'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 tramite policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione

ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di 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 AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. 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'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate sulle identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni 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 incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. 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 allegare 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 allegata 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 è possibile utilizzare le policy gestite da AWSda IAM in una policy basata su 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 sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. 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 altri tipi di policy 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.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli 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. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni 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 informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Funzionamento di Amazon Detective con IAM

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon Detective. Inoltre, non sono in grado di eseguire attività utilizzando l'API AWS Management Console, AWS CLI, o AWS. Un amministratore di Detective deve avere policy AWS Identity and Access Management (IAM) che concedono a utenti e ruoli IAM l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy al principale che richiedono tali autorizzazioni.

Detective utilizza le policy basate sull'identità IAM per concedere le autorizzazioni per i seguenti tipi di utenti e operazioni:

- Account amministratore: l'account amministratore è il proprietario di un grafico di comportamento, che utilizza i dati del proprio account. L'account amministratore può invitare gli account membri a contribuire con i propri dati al grafico di comportamento. Inoltre, utilizza il grafico di comportamento per valutare e analizzare i risultati e le risorse associati a tali account.

  È possibile impostare le policy per consentire agli utenti diversi dall'account amministratore di eseguire diversi tipi di attività. Ad esempio, un utente con un account amministratore potrebbe avere solo le autorizzazioni per gestire gli account membri. Un altro utente potrebbe avere solo le autorizzazioni per utilizzare il grafico di comportamento per le indagini.
- Account membri: un account membro è un account invitato a contribuire con i dati a un grafico di comportamento. Un account membro risponde a un invito. Dopo aver accettato un invito, un account membro può rimuovere il proprio account dal grafico di comportamento.

Per ottenere un quadro generale del funzionamento di Detective e di come altri Servizi AWS lavorano con IAM, consulta Creazione di policy sulla scheda JSON nella Guida per l'utente di IAM.

Policy basate su identità di Detective

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Detective supporta operazioni, risorse e chiavi di condizione specifiche.

Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. 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 operazioni di policy hanno spesso lo stesso nome dell'operazione API AWS. 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.

Le istruzioni della policy devono includere un elemento `Action` o un elemento `NotAction`. L'elemento `Action` elenca le azioni consentite dalla policy. L'elemento `NotAction` elenca le operazioni non consentite.

Le operazioni definite per Detective riflettono le attività che è possibile eseguire utilizzando Detective. Le operazioni delle policy in Detective hanno il seguente prefisso: `detective:`.

Ad esempio, per concedere l'autorizzazione per utilizzare l'operazione API `CreateMembers` per invitare gli account membri a un grafico di comportamento, includi l'operazione `detective:CreateMembers` nella policy.

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Ad esempio, per un account membro, la politica include l'insieme di operazioni relative alla gestione di un invito:

```
"Action": [
      "detective:ListInvitations",
```

```
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

Per specificare più operazioni, è possibile utilizzare i caratteri jolly (*). Ad esempio, per gestire i dati utilizzati nel grafico di comportamento, gli account amministratore in Detective devono poter eseguire le seguenti attività:

- Visualizza l'elenco di account membri (`ListMembers`).
- Ottieni informazioni sugli account membri selezionati (`GetMembers`).
- Invita gli account membri a visualizzare il loro grafico di comportamento (`CreateMembers`).
- Rimuovi i membri dal grafico di comportamento (`DeleteMembers`).

Invece di elencare queste operazioni separatamente, puoi concedere l'accesso a tutte le operazioni che terminano con la parola `Members`. La policy a tal fine potrebbe includere la seguente operazione:

```
"Action": "detective:*Members"
```

Per visualizzare un elenco di operazioni di Detective, consulta Operazioni definite da Amazon Detective nella Guida di riferimento per l'autorizzazione del servizio.

Risorse

Gli amministratori possono utilizzare le policy JSON AWSper specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per ulteriori informazioni sul formato degli ARN, consulta Nome della risorsa Amazon (ARN) e spazi dei nomi del servizio AWS.

Per Detective, l'unico tipo di risorsa è il grafico di comportamento. La risorsa del grafico di comportamento in Detective ha il seguente ARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Ad esempio, un grafico di comportamento ha i seguenti valori:

- La Regione per il grafico di comportamento è `us-east-1`.
- L'ID account per l'account amministratore è `111122223333`.
- L'ID del grafico di comportamento è `027c7c4610ea4aacaf0b883093cab899`.

Per identificare questo grafico di comportamento in una istruzione `Resource`, è necessario utilizzare il seguente ARN:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Per specificare più risorse in una istruzione `Resource`, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Ad esempio, lo stesso account AWS può essere invitato a diventare un account membro in più di un grafico di comportamento. Nella policy per quell'account membro, l'istruzione `Resource` elencherebbe i grafici di comportamento a cui sono stati invitati.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Alcune operazioni di Detective, come la creazione di un grafico di comportamento, la visualizzazione di grafici di comportamento e la visualizzazione degli inviti al grafico di comportamento, non vengono

eseguite su un grafico di comportamento specifico. Per queste operazioni, l'istruzione `Resource` deve utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Per le operazioni dell'account amministratore, Detective verifica sempre che l'utente che effettua la richiesta appartenga all'account amministratore per il grafico di comportamento interessato. Per le operazioni dell'account membro, Detective verifica sempre che l'utente che effettua la richiesta appartenga all'account membro. Anche se una policy IAM concede l'accesso a un grafico di comportamento, se l'utente non appartiene all'account corretto, l'utente non può eseguire l'azione.

Per tutte le operazioni eseguite su uno specifico grafico di comportamento, la policy IAM deve includere l'ARN del grafico. L'ARN del grafico può essere aggiunto in un secondo momento. Ad esempio, quando un account abilita per la prima volta Detective, la policy IAM iniziale fornisce l'accesso a tutte le operazioni di Detective, utilizzando il carattere jolly per l'ARN del grafico. Ciò consente all'utente di iniziare immediatamente a gestire gli account membri e a condurre indagini nel proprio grafico di comportamento. Dopo aver creato il grafico di comportamento, puoi aggiornare la policy per aggiungere l'ARN del grafico.

Chiavi di condizione

Gli amministratori possono utilizzare le policy JSON AWS 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 specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Detective non definisce il proprio set di chiavi di condizione. Supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente IAM.

Per scoprire con quali operazioni e risorse puoi utilizzare una chiave di condizione, consulta Operazioni definite da Amazon Detective.

Esempi

Per visualizzare esempi di policy basate su identità di Detective, consulta Esempi di policy basate sull'identità per Amazon Detective.

Policy basate sulle risorse di Detective (non supportate)

Detective non supporta policy basate su risorse.

Autorizzazione basata sui tag del grafici di comportamento di Detective

A ciascun grafico di comportamento possono essere assegnati valori di tag. È possibile utilizzare questi valori di tag nelle istruzioni condizionali per gestire l'accesso al grafico.

L'istruzione condizionale per un valore di tag utilizza il formato seguente.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Ad esempio, utilizza il codice seguente per consentire o negare un'azione quando il valore del tag `Department` è `Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Per esempi di policy che utilizzano i valori dei tag di risorsa, consulta the section called “Account amministratore: limitazione dell'accesso in base ai valori di tag”.

Ruoli IAM di Detective

Un ruolo IAM è un'entità all'interno dell'account AWS che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Detective

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Per ottenere le credenziali di sicurezza temporanee, esegui una chiamata a operazioni API AWS STS quali, ad esempio, AssumeRole o GetFederationToken.

Detective supporta l'uso di credenziali temporanee.

Ruoli collegati ai servizi

Ruoli collegati al servizio consentono ai servizi AWS di accedere a risorse in altri servizi per completare un'operazione a tuo nome. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi di Detective, consulta the section called “Uso di ruoli collegati ai servizi”.

Ruoli di servizio (non supportati)

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'operazione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Detective non supporta i ruoli del servizio.

Esempi di policy basate sull'identità per Amazon Detective

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse Detective. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, AWS CLI o un'API AWS.

Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o gruppi IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

Best practice delle policy

Le policy basate sulle identità determinano se qualcuno può creare, accedere o eliminare risorse Detective 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:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWSspecifiche 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 a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo 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 al linguaggio 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.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva 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 di IAM.

Utilizzo della console Detective

Per utilizzare la console Amazon Detective, l'utente o il ruolo deve avere accesso alle operazioni pertinenti, che corrispondono alle relative operazioni nell'API.

Per abilitare Detective e diventare un account amministratore per un grafico di comportamento, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `CreateGraph`.

Per utilizzare la console Detective per eseguire operazioni dell'account amministratore, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `ListGraphs`. Ciò concede l'autorizzazione a recuperare i grafici di comportamento di cui il relativo account è amministratore. È inoltre necessario concedergli l'autorizzazione a eseguire operazioni specifiche dell'account amministratore.

Le operazioni più basilari dell'account amministratore consistono nel visualizzare un elenco degli account membri in un grafico di comportamento e nell'utilizzare il grafico di comportamento per le indagini.

- Per visualizzare l'elenco degli account membri in un grafico di comportamento, è necessario concedere al principale l'autorizzazione per l'operazione `ListMembers`.
- Per condurre un'indagine in un grafico di comportamento, è necessario concedere al principale l'autorizzazione per l'operazione `SearchGraph`.

Per utilizzare la console Detective per eseguire operazioni dell'account membro, all'utente o al ruolo deve essere concessa l'autorizzazione per l'operazione `ListInvitations`. Ciò concede l'autorizzazione a visualizzare gli inviti del grafico di comportamento. È quindi possibile concedergli l'autorizzazione per operazioni specifiche dell'account membro.

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 allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLIo l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Account amministratore: gestione degli account membri in un grafico di comportamento

Questa policy di esempio è diretta agli utenti con account amministratore che sono responsabili solo della gestione degli account membri utilizzati nel grafico di comportamento. La policy, inoltre, consente all'utente di visualizzare le informazioni di utilizzo e di disattivare Detective. La policy non concede l'autorizzazione per utilizzare il grafico di comportamento per le indagini.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Account amministratore: utilizzo di un grafico di comportamento per le indagini

Questa policy di esempio è diretta agli utenti con account amministratore che utilizzano il grafico di comportamento solo per le indagini. Non possono visualizzare o modificare l'elenco degli account dei membri nel grafico di comportamento.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

```
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Account membro: gestione degli inviti e delle iscrizioni al grafico di comportamento

Questa policy di esempio è diretta agli utenti che appartengono a un account membro. Nell'esempio, l'account membro appartiene a due grafici di comportamento. La policy concede l'autorizzazione a rispondere agli inviti e rimuovere l'account membro dal grafico di comportamento.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Account amministratore: limitazione dell'accesso in base ai valori di tag

La seguente policy consente all'utente di utilizzare un grafico di comportamento per verificare se il tag `SecurityDomain` del grafico di comportamento corrisponde al tag `SecurityDomain` dell'utente.

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

La seguente policy impedisce agli utenti di utilizzare un grafico di comportamento per verificare se il valore del tag `SecurityDomain` per il grafico di comportamento è `Finance`.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso di Amazon Detective

Utilizza le seguenti informazioni per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Detective e IAM. Se si verificano problemi di accesso rifiutato o problemi simili durante l'utilizzo di AWS Identity and Access Management (IAM), consulta gli argomenti Risoluzione dei problemi relativi a IAM nella Guida per l'utente di IAM.

Non sono autorizzato a eseguire un'operazione in Detective

Se la AWS Management Console indica che non hai l'autorizzazione a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona che ti ha fornito il nome utente e la password.

L'errore di esempio riportato di seguito si verifica quando l'utente `mateojackson` IAM prova a utilizzare la console per accettare un invito a diventare un account membro per un grafico di comportamento, ma non dispone delle autorizzazioni `detective:AcceptInvitation`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `arn:aws:detective:us-east-1:444455556666:graph:567856785678` utilizzando l'operazione `detective:AcceptInvitation`.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Detective.

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` prova a utilizzare la console per eseguire un'operazione in Detective. 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`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire alle persone esterne al mio account AWS di accedere alle mie risorse Detective

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 Detective supporta queste funzionalità, consulta Funzionamento di Amazon Detective con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli 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, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo dei ruoli collegati ai servizi per Detective

Amazon Detective utilizza ruoli collegati ai servizi di AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente a Detective. I ruoli collegati ai servizi sono predefiniti da Detective e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Detective perché consente di evitare l'aggiunta manuale delle autorizzazioni necessarie. Detective definisce le autorizzazioni dei relativi ruoli collegati ai servizi e, salvo diversamente definito, solo Detective 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.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Detective perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione relativa ai Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli un Sì con un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per Detective

Detective usa il ruolo collegato ai servizi denominato AWSServiceRoleForDetective che consente a Detective di accedere alle informazioni su AWS Organizations per tuo conto.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForDetective considera attendibili i seguenti servizi:

- `detective.amazonaws.com`

Il ruolo collegato ai servizi AWSServiceRoleForDetective utilizza la policy gestita `AmazonDetectiveServiceLinkedRolePolicy`.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Detective

Non è necessario creare manualmente un ruolo collegato ai servizi. Quando si definisce l'account amministratore di Detective per un'organizzazione nella AWS Management Console, la AWS CLI o l'API AWS, Detective crea il ruolo collegato ai servizi per tuo conto.

Se elimini questo ruolo collegato al servizio, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando si definisce l'account amministratore di Detective per un'organizzazione, Detective crea il ruolo collegato ai servizi per tuo conto.

Modifica di un ruolo collegato ai servizi per Detective

Detective non consente di modificare il ruolo collegato ai servizi AWSServiceRoleForDetective. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità

potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Detective

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Detective utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Eliminare le risorse Detective utilizzate da AWSServiceRoleForDetective

1. Rimuovi l'account amministratore di Detective. Per informazioni, consultare the section called “Designazione dell'account amministratore di Detective”.
2. Ripeti la procedura in ogni Regione in cui hai designato l'account amministratore di Detective.

Eliminazione manuale del ruolo collegato al servizio con IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato al servizio AWSServiceRoleForDetective. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Detective

Detective supporta l'utilizzo di ruoli collegati ai servizi in tutte le Regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Policy gestite da AWS per Amazon Detective

Una policy gestita da AWSè una policy autonoma creata e amministrata da AWS. Le policy gestite da AWSsono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWSpotrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWSaggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWSaggiorni una policy gestita da AWSquando viene lanciato un nuovo Servizio AWSo nuove operazioni API diventano disponibili per i servizi esistenti.

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

AWSPolicy gestita: AmazonDetectiveFullAccess

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

Questa policy concede autorizzazioni amministrative che consentono a un principale l'accesso completo a tutte le operazioni di Amazon Detective. Puoi collegare questa policy a un principale prima che abiliti Detective per il suo account. Deve inoltre essere collegato al ruolo utilizzato per eseguire gli script Python di Detective per creare e gestire un grafico del comportamento.

I principali con queste autorizzazioni possono gestire gli account membri, aggiungere tag al loro grafico del comportamento e utilizzare Detective per le indagini. Possono anche archiviare i risultati di GuardDuty. La policy fornisce le autorizzazioni necessarie alla console Detective per visualizzare i nomi degli account presenti in AWS Organizations.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai principali l'accesso completo alle operazioni di Detective.
- `organizations`: consente ai principali di recuperare informazioni sugli account di un'organizzazione da AWS Organizations. Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account.

- `guardduty`: consente ai principali di ottenere e archiviare i risultati di GuardDuty dall'interno di Detective.
- `securityhub`: consente ai principali di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
```

```
}
```

AWSPolicy gestita: AmazonDetectiveMemberAccess

Puoi collegare la policy `AmazonDetectiveMemberAccess` anche alle tue entità IAM.

Questa policy fornisce ai membri l'accesso ad Amazon Detective e l'accesso in ambito alla console.

Con questa policy, puoi:

- Visualizzare gli inviti all'iscrizione al grafico di Detective e accetta o rifiuta tali inviti.
- Scoprire come la tua attività in Detective contribuisce ai costi di utilizzo di questo servizio nella pagina Utilizzo.
- Annullare la tua appartenenza a un grafico.

Questa policy concede le autorizzazioni di sola lettura che consentono l'accesso in ambito alla console di Detective.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai membri di accedere a Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
```

```
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSPolicy gestita: AmazonDetectiveInvestigatorAccess

Puoi collegare la policy `AmazonDetectiveInvestigatorAccess` anche alle tue entità IAM.

Questa policy fornisce ai responsabili delle indagini l'accesso al servizio Detective e l'accesso in ambito alle dipendenze dell'interfaccia utente della console Detective. Questa policy concede le autorizzazioni per abilitare le indagini di Detective per gli utenti IAM e i ruoli IAM. Puoi indagare per identificare gli indicatori di compromissione, come i risultati, utilizzando un report di indagine, che fornisce analisi e approfondimenti sugli indicatori di sicurezza. Il report è classificato in base alla gravità, determinata utilizzando l'analisi comportamentale e il machine learning di Detective. Puoi utilizzare il report per dare priorità alla riparazione delle risorse.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai responsabili delle indagini di accedere alle operazioni di Detective, di abilitare le indagini di Detective e di abilitare il riepilogo dei gruppi di risultati.
- `guardduty`: consente ai principali di ottenere e archiviare i risultati di GuardDuty dall'interno di Detective.
- `securityhub`: consente ai principali di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.
- `organizations`: consente ai principali di recuperare informazioni sugli account di un'organizzazione da AWS Organizations. Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
```

```
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy gestita da AWS: AmazonDetectiveOrganizationsAccess

Puoi collegare la policy `AmazonDetectiveOrganizationsAccess` anche alle tue entità IAM.

Questa policy concede l'autorizzazione per abilitare e gestire Amazon Detective all'interno di un'organizzazione. È possibile abilitare Detective in tutta l'organizzazione e determinare l'account amministratore delegato per Detective.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `detective`: consente ai principali di accedere alle operazioni di Detective.
- `iam`: specifica che un ruolo collegato ai servizi viene creato quando Detective chiama `EnableOrganizationAdminAccount`.
- `organizations`: consente ai principali di recuperare informazioni sugli account di un'organizzazione da AWS Organizations. Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Detective di visualizzare i nomi degli account oltre ai numeri di account. Consente l'integrazione di un servizio AWS, consente la registrazione e l'annullamento della registrazione dell'account membro specificato come amministratore delegato e

consente ai principali di recuperare gli account amministratore delegato in altri servizi di sicurezza come Amazon Detective, Amazon GuardDuty, Amazon Macie e AWS Security Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWSPolicy gestita: AmazonDetectiveServiceLinkedRole

Non è possibile allegare la policy `AmazonDetectiveServiceLinkedRole` alle entità IAM. Questa policy è collegata a un ruolo collegato ai servizi che consente a Detective di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta the section called “Uso di ruoli collegati ai servizi”.

Questa policy concede le autorizzazioni amministrative che consentono al ruolo collegato ai servizi di recuperare le informazioni sull'account per un'organizzazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations`: recupera le informazioni sull'account di un'organizzazione.

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

Aggiornamenti di Detective alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per Detective a partire da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti.

Modifica	Description	Data
AmazonDetectiveInvestigatorAccess: aggiornamento a policy esistenti	Sono state aggiunte operazioni di riepilogo dei gruppi di risultati e indagini di Detective alla policy `AmazonDetectiveInvestigatorAccess` . Queste operazioni consentono di avviare, recuperare e aggiornare le indagini di Detective e ottenere un riepilogo dei gruppi di risultati all'interno di Detective.	26 novembre 2023

Modifica	Description	Data
AmazonDetectiveFullAccess e AmazonDetectiveInvestigatorAccess: aggiornamenti alle policy esistenti	Detective ha aggiunto operazioni `GetFindings` di Centrale di sicurezza alle policy `AmazonDetectiveFullAccess` e `AmazonDetectiveInvestigatorAccess`. Queste operazioni consentono di ottenere i risultati di Centrale di sicurezza dall'interno di Detective.	16 maggio 2023
AmazonDetectiveOrganizationsAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveOrganizationsAccess`. Questa policy concede l'autorizzazione per abilitare e gestire Detective all'interno di un'organizzazione	2 marzo 2023
AmazonDetectiveMemberAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveMemberAccess`. Questa policy fornisce ai membri l'accesso a Detective e l'accesso in ambito alle dipendenze dell'interfaccia utente della console.	17 gennaio 2023

Modifica	Description	Data
AmazonDetectiveFullAccess: aggiornamenti a una policy esistente	Detective ha aggiunto le operazioni `GetFindings` GuardDuty alla policy `AmazonDetectiveFullAccess` . Queste operazioni consentono di ottenere i risultati di GuardDuty dall'interno di Detective.	17 gennaio 2023
AmazonDetectiveInvestigatorAccess: nuova policy	Detective ha aggiunto la policy `AmazonDetectiveInvestigatorAccess` . Questa policy consente al principale di condurre indagini in Detective.	17 gennaio 2023
AmazonDetectiveServiceLinkedRole: nuova policy	Detective ha aggiunto una nuova policy per il suo ruolo collegato ai servizi. La policy consente al ruolo collegato ai servizi di recuperare informazioni sugli account in un'organizzazione.	16 dicembre 2021
Detective ha iniziato a tenere traccia delle modifiche	Detective ha iniziato a monitorare le modifiche per le sue policy gestite da AWS.	10 maggio 2021

Registrazione e monitoraggio in Amazon Detective

Amazon Detective è integrato in AWS CloudTrail. CloudTrail acquisisce tutte le chiamate API per Detective come eventi.

Per i dettagli sull'utilizzo della registrazione di CloudTrail per Detective, consulta the section called “Registrazione delle chiamate API di Detective con CloudTrail”.

Convalida della conformità per Amazon Detective

Amazon Detective rientra nell'ambito del programma di garanzia AWS. Per ulteriori informazioni, consulta Health Information Trust Alliance Common Security Framework (HITRUST) CSF.

Per un elenco dei servizi AWS coperti da programmi di conformità specifici, consulta Servizi AWS coperti dal programma di compliance. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download dei report in AWS Artifact.

AWS offre le risorse seguenti per facilitare la conformità:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config - Il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub - Questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza in Amazon Detective

L'infrastruttura globale di AWS è basata su Regioni e zone di disponibilità AWS. AWS Le Regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le Zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico 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.

Per ulteriori informazioni sulle Regioni AWS e sulle zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale AWS, Detective utilizza la resilienza integrata in Amazon DynamoDB e Amazon Simple Storage Service (Amazon S3).

L'architettura di Detective è inoltre resistente al fallimento di una singola zona di disponibilità. Questa resilienza è integrata in Detective e non richiede alcuna configurazione.

Sicurezza dell'infrastruttura in Amazon Detective

In qualità di servizio gestito, Amazon Detective è protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere a Detective tramite 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. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Best practice di sicurezza per Amazon Detective

Detective fornisce una serie di funzionalità di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché potrebbero non essere appropriate o sufficienti per il tuo ambiente, prendile come considerazioni utili più che istruzioni.

Per Detective, le best practice di sicurezza sono associate alla gestione degli account in un grafico di comportamento.

Best practice per gli account amministratore

Quando inviti gli account membri a visualizzare il tuo grafico di comportamento, invita solo gli account controllati da te.

Limita l'accesso al grafico di comportamento. Quando un utente ha accesso a un grafico di comportamento, può visualizzare tutti i risultati relativi agli account membri. Tali risultati potrebbero rivelare informazioni di sicurezza sensibili.

Best practice per gli account membri

Quando ricevi un invito a visualizzare un grafico di comportamento, assicurati di verificare la fonte dell'invito.

Controlla l'identificatore dell'account AWS dell'account amministratore che ha inviato l'invito. Assicurati di sapere a chi appartiene l'account e verifica che l'account che ha inviato l'invito abbia un motivo legittimo per monitorare i tuoi dati di sicurezza.

Disabilitazione di Amazon Detective

L'account amministratore per un grafico di comportamento può disabilitare Amazon Detective dalla console Detective, dall'API Detective o dalla AWS Command Line Interface. Quando disabiliti Detective, il grafico di comportamento e i dati di Detective associati vengono eliminati.

Una volta eliminato, il grafico di comportamento non può più essere ripristinato.

Indice

Disabilitazione di Detective (console)

Puoi disabilitare Amazon Detective dalla AWS Management Console.

Disabilitare Detective (console)

1. Apri la console Amazon Detective all'indirizzo https://console.aws.amazon.com/detective/.
2. Nel riquadro di navigazione di Detective, in Impostazioni, scegli Generale.
3. Nella pagina Generale, in Disabilita Detective, scegli Disabilita Detective.
4. Quando richiesto, digita **`disable`** per confermare.
5. Scegli Disabilita Detective.

Disabilitazione di Detective (API Detective, AWS CLI)

Puoi disabilitare Amazon Detective dall'API Detective o dalla AWS Command Line Interface. Per ottenere l'ARN del grafico del comportamento da utilizzare nella richiesta, utilizza l'operazione `ListGraphs`.

Disabilitare Detective (API Detective, AWS CLI)

- API Detective: usa l'operazione `DeleteGraph`. È necessario specificare l'ARN del grafico.
- AWS CLI: alla riga di comando, esegui il comando `delete-graph`.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Esempio:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Disabilitazione di Detective tra le Regioni (script Python su GitHub)

Detective fornisce uno script open source in GitHub che consente di disabilitare Detective per un account amministratore in un elenco specifico di Regioni.

Per informazioni su come configurare e utilizzare gli script di GitHub, consulta Utilizzo degli script Python di Amazon Detective.

Utilizzo degli script Python di Amazon Detective

Amazon Detective fornisce un set di script Python open source nel repository GitHub amazon-detective-multiaccount-scripts. Gli script richiedono Python 3.

Puoi utilizzarli per completare le attività seguenti:

- Abilita Detective per un account amministratore in tutte le Regioni.

  Quando abiliti Detective, puoi assegnare i valori dei tag al grafico di comportamento.
- Aggiungi gli account membri ai grafici di comportamento di un account amministratore in tutte le Regioni.
- Facoltativamente, invia le e-mail di invito agli account membri. Puoi anche configurare la richiesta per non inviare e-mail di invito.
- Rimuovi gli account membri dai grafici di comportamento di un account amministratore in tutte le Regioni.
- Disabilita Detective per un account amministratore in tutte le Regioni. Quando un account amministratore disabilita Detective, il grafico di comportamento dell'account amministratore in ciascuna Regione viene disabilitato.

Panoramica dello script `enableDetective.py`

Lo script `enableDetective.py` svolge le seguenti funzioni:

1. Abilita Detective per un account amministratore in ogni Regione specificata, se l'account amministratore non ha già abilitato Detective in quella Regione.

   Quando utilizzi lo script per abilitare Detective, puoi assegnare i valori dei tag al grafico di comportamento.
2. Facoltativamente, invia gli inviti dall'account amministratore agli account membri specificati per ogni grafico di comportamento.

   I messaggi e-mail di invito utilizzano il contenuto predefinito dei messaggi e non possono essere personalizzati.

   Puoi anche configurare la richiesta per non inviare e-mail di invito.
3. Accetta automaticamente gli inviti per gli account membri.

Poiché lo script accetta automaticamente gli inviti, gli account membri possono ignorare questi messaggi.

Ti consigliamo di contattare direttamente gli account membri per avvisarli che gli inviti vengono accettati automaticamente.

Panoramica dello script `disableDetective.py`

Lo script `disableDetective.py` elimina gli account dei membri specificati dai grafici di comportamento dell'account amministratore nelle Regioni specificate.

Fornisce inoltre un'opzione per disabilitare Detective per l'account amministratore nelle Regioni specificate.

Autorizzazioni richieste per gli script

Gli script richiedono un ruolo AWS pre-esistente nell'account amministratore e in tutti gli account membri aggiunti o rimossi.

> **Note**
>
> Il nome del ruolo deve essere lo stesso in tutti gli account.

Le best practice consigliate della policy IAM prevedono l'utilizzo di ruoli con meno ambito. Per eseguire il flusso di lavoro dello script che prevede la creazione di un grafico, la creazione di membri e l'aggiunta di membri al grafico, le autorizzazioni richieste sono:

- detective:CreateGraph
- detective:CreateMembers
- detective:DeleteGraph
- detective:DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

Relazione di attendibilità del ruolo

La relazione di attendibilità tra i ruoli deve consentire all'istanza o alle credenziali locali di assumere il ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se non disponi di un ruolo comune che includa le autorizzazioni richieste, devi creare un ruolo con almeno tali autorizzazioni in ogni account membro. È inoltre necessario creare il ruolo nell'account amministratore.

Quando crei il ruolo, assicurati di completare le seguenti operazioni:

- Usa lo stesso nome di ruolo in ogni account.
- Aggiungi le autorizzazioni richieste sopra (consigliate) o seleziona la policy gestita AmazonDetectiveFullAccess.
- Aggiungi il blocco di relazioni di attendibilità tra ruoli come discusso in precedenza.

Per automatizzare questo processo, puoi utilizzare il modello `EnableDetective.yaml` AWS CloudFormation. Poiché il modello crea solo risorse globali, può essere eseguito in qualsiasi Regione.

Configurazione dell'ambiente di esecuzione per gli script Python

Puoi eseguire gli script da un'istanza EC2 o dal tuo computer locale.

Avvio e configurazione di un'istanza EC2

Un'opzione per eseguire gli script è eseguirli da un'istanza EC2.

Avvio e configurazione di un'istanza EC2

1. Avvia un'istanza EC2 nel tuo account amministratore. Per maggiori dettagli su come avviare un'istanza EC2, consulta Nozioni di base sulle istanze Amazon EC2 Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.
2. Collega all'istanza un ruolo IAM con le autorizzazioni necessarie per consentire all'istanza di effettuare chiamate a `AssumeRole`all'interno dell'account amministratore.

   Se hai utilizzato il modello `EnableDetective.yaml` AWS CloudFormation, allora è stato creato un ruolo di istanza con un profilo denominato `EnableDetective`.

   Altrimenti, per informazioni sulla creazione di un ruolo di istanza, consulta il post del blog Sostituisci o collega facilmente un ruolo IAM a un'istanza EC2 esistente utilizzando la console EC2.
3. Installa il software richiesto:
   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (versione minima 1.15): `sudo pip install boto3`
4. Clona il repository sull'istanza EC2.

   ```
   git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
   ```

Configurazione di un computer locale per eseguire gli script

È inoltre possibile eseguire gli script dal computer locale.

Configurare un computer locale per eseguire gli script

1. Assicurati di aver configurato sul tuo computer locale le credenziali per il tuo account amministratore che dispone dell'autorizzazione per chiamare `AssumeRole`.
2. Installa il software richiesto:
   - Python 3
   - Boto (versione minima 1.15)
   - Script GitHub

Piattaforma	Istruzioni di configurazione
Windows	1. Installa Python 3 (https://www.python.org/downloads/windows/). 2. Apri un prompt dei comandi. 3. Per installare Boto, esegui: `pip install boto3` 4. Scarica il codice sorgente dello script da GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Mac	1. Installa Python 3 (https://www.python.org/downloads/mac-osx/). 2. Apri un prompt dei comandi. 3. Per installare Boto, esegui: `pip install boto3` 4. Scarica il codice sorgente dello script da GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	1. Per installare Python 3, esegui uno dei comandi riportati: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Per installare Boto, esegui: `sudo pip install boto3` 3. Clona il codice sorgente dello script da https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Creazione di un elenco `.csv` di account membri da aggiungere o rimuovere

Per identificare gli account membro da aggiungere o rimuovere dai grafici di comportamento, fornisci un file `.csv` contenente l'elenco degli account.

Ogni account viene riportato su una riga separata. Ogni voce dell'account membro contiene l'ID account AWS e l'indirizzo e-mail dell'utente root dell'account.

Fai riferimento al file di esempio seguente:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Esecuzione di **enableDetective.py**

Puoi eseguire lo script `enableDetective.py` da un'istanza EC2 o dal tuo computer locale.

Per eseguire **enableDetective.py**

1. Copia il file `.csv` nella directory `amazon-detective-multiaccount-scripts` dell'istanza EC2 o del computer locale.
2. Passare alla directory `amazon-detective-multiaccount-scripts`.
3. Eseguire lo script `enableDetective.py`.

   ```
   enableDetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
   disable_email
   ```

Quando esegui lo script, sostituisci i seguenti valori:

administratorAccountID

L'ID account AWS per l'account amministratore.

roleName

Il nome del ruolo AWS da assumere nell'account amministratore e in ogni account membro.

inputFileName

Il nome del file `.csv` contenente l'elenco degli account membri da aggiungere ai grafici di comportamento dell'account amministratore.

tagValueList

(Facoltativo) Un elenco di valori di tag separati da virgole da assegnare a un nuovo grafico di comportamento.

Per ogni valore di tag, il formato è *key*=*value*. Ad esempio:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Facoltativo) Un elenco separato da virgole di Regioni in cui aggiungere gli account membri al grafico di comportamento dell'account amministratore. Ad esempio:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

L'account amministratore potrebbe non avere già abilitato Detective in una Regione. In tal caso, lo script abilita Detective e crea un nuovo grafico di comportamento per l'account amministratore.

Se non fornisci un elenco di Regioni, lo script agirà su tutte le Regioni supportate da Detective.

`--disable_email`

(Facoltativo) Se inclusa, Detective non invia e-mail di invito agli account membri.

Esecuzione di **disableDetective.py**

Puoi eseguire lo script `disableDetective.py` da un'istanza EC2 o dal tuo computer locale.

Per eseguire **disableDetective.py**

1. Copia i file `.csv` nella directory `amazon-detective-multiaccount-scripts`.
2. Per utilizzare il file `.csv` per eliminare gli account membri elencati dai grafici di comportamento dell'account amministratore in un elenco specificato di Regioni, esegui lo script `disableDetective.py` come segue:

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList
   ```

3. Per disabilitare Detective per l'account amministratore in tutte le Regioni, esegui lo script `disableDetective.py` con il flag `--delete-master`.

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList --delete_master
   ```

Quando esegui lo script, sostituisci i seguenti valori:

administratorAccountID

L'ID account AWS per l'account amministratore.

roleName

Il nome del ruolo AWS da assumere nell'account amministratore e in ogni account membro.

inputFileName

Il nome del file `.csv` contenente l'elenco degli account membri da rimuovere dai grafici di comportamento dell'account amministratore.

Devi fornire un file `.csv` anche se stai disabilitando Detective.

regionList

(Facoltativo) Un elenco separato da virgole di Regioni in cui completare una delle seguenti operazioni:

- Rimuovi gli account membri dai grafici di comportamento dell'account amministratore.
- Se il flag `--delete-master` è incluso, disabilita Detective.

Ad esempio:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Se non fornisci un elenco di Regioni, lo script agirà su tutte le Regioni supportate da Detective.

Cronologia dei documenti per la Guida all'amministrazione di Detective

Nella tabella seguente vengono descritte le modifiche importanti apportate alla documentazione dall'ultima versione di Detective. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

- Ultimo aggiornamento della documentazione: 15 aprile 2024

Modifica	Descrizione	Data
Aggiornamento della documentazione	Il contenuto dell'Amazon Detective Administration Guide è ora consolidato nella Amazon Detective User Guide. Amazon Detective Administration Guide raggiungerà la fine del supporto standard l'8 maggio 2024.	15 aprile 2024
Rimosso il requisito di GuardDuty iscrizione ad Amazon	Non è più necessario essere un GuardDuty cliente per abilitare Amazon Detective. Il requisito che doveva essere GuardDuty abilitato nel tuo account per 48 ore prima di abilitare Detective è stato rimosso.	2 febbraio 2024
Modifiche nel modo in cui Detective legge il flusso di traffico per i VPC condivisi	Se utilizzi un Amazon VPC condiviso, potresti notare cambiamenti nel traffico monitorato da Detective. Ti consigliamo di esaminare le modifiche nei Dettagli dell'attività per il volume globale dei	20 dicembre 2023

	flussi VPC per comprende re i potenziali effetti sulla copertura e di esaminare Come Amazon Detective calcola il costo previsto per comprendere l'impatto sui costi del servizio.	
Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Sono state aggiunte operazion i di riepilogo dei gruppi di risultati e indagini di Detective alla policy `AmazonDet ectiveInvestigator Access` .	26 novembre 2023
Endpoint e quote di Amazon Detective	Detective è ora disponibile nella Regione Israele (Tel Aviv).	25 agosto 2023
Aggiunti risultati AWS di sicurezza come nuovo pacchetto opzionale di sorgenti dati.	Detective ora fornisce risultati AWS di sicurezza come pacchetto di sorgenti dati opzionale. Questo pacchetto di origini dati facoltativi consente a Detective di importare dati da Centrale di sicurezza e di aggiungerli al grafico di comportamento.	16 maggio 2023
Aggiunti nuovi pannelli nella console di Detective per aiutare gli utenti a seleziona re la policy gestita da AWS appropriata per il caso d'uso specifico.	Detective offre policy gestite per scegliere in modo sicuro le autorizzazioni di cui si ha bisogno.	3 aprile 2023

Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Il Detective ora supporta le azioni GuardDuty per ottenere risultati attravers o la AmazonDetectiveFul lAccess polizza. Il capitolo sulla sicurezza ora fornisce dettagli sulle seguenti nuove politiche gestite per Detective : AmazonDetectiveMem berAccess e AmazonDet ectiveInvestigatorAccess.	17 gennaio 2023
Aggiunta la conservazione dei dati	Con Detective puoi accedere fino a un anno di dati storici degli eventi.	20 dicembre 2022
Aggiunti termini relativi ai gruppi di risultati	Detective ora supporta gruppi di risultati che collegano i risultati correlati in un'unica visualizzazione per indagare su potenziali attività dannose nel tuo ambiente. Da un profilo del gruppo di risultati, puoi passare ai profili di entità e alle panoramiche dei risultati relative a quel gruppo.	3 agosto 2022

Aggiunta una nuova origine dati facoltativa	Detective ora supporta i log di controllo EKS come pacchetto di origini dati facoltative. Un account amministratore può abilitare questa nuova origine dati per il grafico di comportamento esistente. Nei grafici creati dopo questa data questa origine dati sarà abilitata per impostazione predefinita. Gli amministratori possono disabilitare questa origine dati manualmente in qualsiasi momento.	26 luglio 2022
Nuovo ruolo collegato ai servizi e policy gestita per Detective	Detective ha ora un ruolo collegato ai servizi, `AWSServiceRoleForDetective` . Il ruolo collegato ai servizi viene utilizzato per accedere ai dati di Organizations per tuo conto. Il ruolo utilizza una nuova policy gestita da `AmazonDetectiveServiceLinkedRolePolicy` .	16 dicembre 2021

È stata aggiunta l'integrazione con AWS Organizations	Detective è ora integrato con Organizations. L'account di gestione dell'organizzazione designa un account amministratore di Detective per l'organizzazione. L'account amministratore di Detective può visualizzare tutti gli account dell'organizzazione e abilitarli come account membri nel grafico di comportamento dell'organizzazione.	16 dicembre 2021
Aggiornati i valori per le quote di volume dei dati del grafico di comportamento	Sono state aumentate le quote di volume di dati per i grafici di comportamento. Con 3,24 TB al giorno, Detective emette un avviso. Con 3,6 TB al giorno, non è possibile aggiungere nuovi account. Con 4,5 TB al giorno, Detective interrompe l'importazione dei dati nel grafico di comportamento.	10 giugno 2021
Aggiunti valori di tag alle opzioni dello script Python	Quando si utilizza lo script Python di Detective `enableDetective.py` per abilitare Detective, puoi assegnare i valori dei tag al grafico di comportamento.	19 maggio 2021

Aggiunta l'abilitazione automatica degli account membri che superano il controllo del volume di dati	Quando gli account membri accettano un invito, il loro stato è Accettato (Non abilitato) fino a quando Detective non verifica che i loro dati non facciano sì che il volume di dati del grafico di comportam ento superi la quota. Se il volume di dati non è un problema, Detective modifica automaticamente lo stato in Accettato (Abilitato). Tieni presente che gli account membri esistenti che si trovano nello stato Accettato (Non abilitati) non possono essere abilitati automatic amente.	12 maggio 2021
Aggiunte informazioni sulla policy gestita al capitolo sulla sicurezza	Una nuova sezione del capitolo sulla sicurezza fornisce dettagli sulle policy gestite per Detective. Detective attualmente fornisce un'unica policy gestita, `AmazonDetectiveFul lAccess` .	10 maggio 2021
Modificati i valori del volume di dati nell'elenco degli account membri	Nella pagina di gestione dell'account, l'elenco degli account membri ora mostra il volume di dati giornaliero per ogni account membro. In precedenza l'elenco mostrava il volume come percentuale del volume totale consentito.	29 aprile 2021

Opzioni riviste per la gestione degli account membri	Il menu Gestisci account è stato sostituito con un menu Operazioni. Combinate le opzioni per aggiungere singoli account e aggiungere account da un file .csv. L'opzione Abilita account è stata spostata da Gestisci account in un'opzione separata accanto a Operazioni.	5 aprile 2021
Aggiunti tag del grafico di comportamento e autorizzazioni basati sui tag	Quando abiliti Detective, puoi aggiungere tag al grafico di comportamento. Puoi gestire i tag per un grafico di comportamento dalla pagina Generale. Detective supporta anche l'autorizzazione basata sui valori dei tag.	31 marzo 2021
Aggiunte differenze per AWS GovCloud (US) le regioni	Detective è ora disponibile nelle AWS GovCloud (US) Regioni. Negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali, Detective non invia e-mail di invito agli account dei membri. Detective, inoltre, non rimuove automaticamente gli account membri che vengono chiusi in AWS.	24 marzo 2021

Aggiunte le schede per filtrare l'elenco degli account membri in base allo stato dell'account membro	L'elenco degli account membri ora mostra delle schede che puoi utilizzare per filtrare l'elenco in base allo stato dell'account membro. È possibile visualizzare tutti gli account membro, quelli con lo stato Accettato (Abilitato) o quelli con uno stato diverso da Accettato (Abilitato).	16 marzo 2021
Aggiunta l'opzione allo script Python per sopprimere le e-mail di invito	Lo script `enableDetective.py` di Detective ora offre un'opzione `--disable_email` . Quando includi questa opzione, Detective non invia e-mail di invito agli account membri.	26 febbraio 2021
Il termine "account principale" è stato modificato in "account amministratore"	Il termine "account principale" viene modificato in "account amministratore". Il termine è cambiato anche nella console e nell'API di Detective.	25 febbraio 2021
Aggiunta l'opzione API per non inviare e-mail di invito agli account membri	Quando si utilizza l'API Detective per aggiungere account membri, gli account amministratore possono scegliere di non inviare e-mail di invito agli account membri.	25 febbraio 2021

La quota degli account membri è stata aumentata a 1.200	Gli account master possono ora invitare fino a 1.200 account membri al proprio grafico di comportamento. In precedenza, questa quota era 1.000.	11 dicembre 2020
Valori aggiunti per le quote di volume dei dati del grafico di comportamento	Aggiornate le informazioni sulle quote di volume dei dati del grafico di comportamento per aggiungere i valori di quota specifici.	11 dicembre 2020
Gli account membri possono ora vederne l'utilizzo e i costi previsti	Gli account membri possono ora visualizzare le informazioni sul proprio utilizzo. Per gli account membri, la pagina Utilizzo mostra la quantità di dati importati in ogni grafico di comportamento a cui contribuiscono. Gli account membri possono inoltre visualizzare il costo previsto per 30 giorni.	26 maggio 2020
La prova gratuita è ora disponibile per account anziché per grafico di comportamento	Ogni account Amazon Detective ora riceve una prova gratuita separata all'interno di ciascuna Regione. La prova gratuita inizia quando l'account abilita Detective o la prima volta che l'account viene abilitato come account membro.	26 maggio 2020

Nuovi script Python open source su GitHub	Il nuovo amazon-detective-multiaccount-scriptsrepository GitHub fornisce script Python open source che è possibile utilizzare per gestire i grafici comportamentali tra le regioni. È possibile abilitare Detective , aggiungere account membri, rimuovere account membri e disabilitare Detective.	21 gennaio 2020
Introduzione di Amazon Detective	Detective utilizza il machine learning e le visualizzazioni dedicate per aiutarti ad analizzare e indagare sui problemi di sicurezza nei carichi di lavoro di Amazon Web Services (AWS).	2 dicembre 2019

Il contenuto dell'Amazon Detective Administration Guide è ora consolidato nella Amazon Detective User Guide. Amazon Detective Administration Guide raggiungerà la fine del supporto standard l'8 maggio 2024.

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.